Shhhhh….It's a Secret: Learning the Key to Cryptography

http://cryptography2014.weebly.com/

Top Secret Picture: Some rights reserved by Malakhi Helel Creative Commons license BY-ND 2.0

Establishing the Mission
More Tools in Your Cryptographic Toolkit
Cracking the Code
The Key to Keeping the Secret

Unit Blurb:

Have you ever wanted to keep a secret and share it only with specific people? Did you use a special code to communicate with your friends so no one else would know what you were saying? In this AIG camp session, you will learn about creating and breaking many types of codes and ciphers used throughout history and take a shot at creating your own secret code or cipher. Are you up for the challenge?

Unit Essential Question
How could you create a perfect cryptosystem?

Nancy Heiniger
Carol Tuttle
SPED 6402 Spring 2014
East Carolina University

CONTENT RESEARCH PAPER

Cryptography, "the art of writing messages with hidden meaning" (Blackwood, 2009, p.5), has been used to keep sensitive information private for centuries. To keep messages secret, cryptographers use transposition and substitution to create codes and ciphers (Janeczko, 2004). Although it was first used for military and political purposes (which are still important), since the use of computers and the internet has become prevalent, the field of cryptography has expanded to include uses important to ordinary people (Blackwood, 2009). While it is still important to securely send messages (Eskicioglu & Litwin, 2001), now, in addition to encryption issues, cryptography addresses issues related to secrecy, data integrity, authenticity, and user identification (K. Gopalakrishnan, personal communication, January 17, 2014).

Fundamentals and Vocabulary

Cryptographers use codes (wherein each word or phrase in a message is replaced by another word, phrase, or set of symbols) and ciphers (wherein each letter in the message is replaced by another letter or symbol) (Janeczko, 2004). These codes and ciphers are used to change plaintext, the message written normally, to ciphertext, the enciphered or encoded text. Two basic strategies, transposition and substitution, can be used alone or in combination to conceal a message (Blackwood, 2009). In opposition to cryptography, cryptanalysis is "the art of figuring out [the] secret meanings" of messages (Blackwood, 2009, p. 5). Because of these two opposing forces, cryptography can be seen as an ongoing game between code makers and code breakers (K. Gopalakrishnan, personal communication, January 17, 2014).

Codes

The simplest use of cryptography involves codes (Janeczko, 2004). While there are non-secret codes (such as zip codes or area codes), cryptographers use secret codes to conceal sensitive information. In order for a code system to work, the code sender and receiver must have a common code book that lists, in a systematic manner, the plaintext words and their ciphertext equivalent. These code books could be created, or they could be books that already exist, like a dictionary (Janeczko, 2004). The advantage of using codes is that it is easy to use the code book to look up the plaintext or ciphertext in order to encode or decode a message. However, this code book must be large enough to contain all the words an encoder would need (which would make it cumbersome to transport), and it could be lost, stolen, or seen by someone who should not see it. In that case, the code would be useless (Janeczko, 2004). Even James Madison experienced a problem with codes in 1793 when he was unable to decode a message Thomas Jefferson sent to him since Madison did not have his code book with him (Beissinger & Pless, 2006).

In addition to written codes, there are spoken codes. Written down, these codes are easy to break, but when spoken, they can confuse others. Spoken codes include the Navajo code used during World War II (which was never broken), Pig Latin, and Turkish Irish (Janeczko, 2004).

Ciphers

Cryptographers also use ciphers. Since ciphers involve enciphering each letter of the plaintext, Morse Code is not a code; it is a non-secret cipher (Blackwood, 2009). Cipher systems have two parts—an algorithm (a mathematical formula to convert the plaintext) and a key (a set of numbers and characters) (Romney, 1998). In a book published in 1883, Auguste Kerckhoffs, a Dutch linguist, stated that the viability of a cipher should not rely on a secret algorithm; as long as the key is secret, an adversary would be unable to read enciphered text (Blackwood, 2009). According to Blackwood (2009), "Even in the computer age, Kerckhoffs's principle remains the fundamental rule of cryptography" (p. 103). In contrast to codes, cipher keys can be memorized so no book is necessary. It is also easier to create a new cipher than to create a new code book if the cipher or code is compromised (Janeczko, 2004).

Transposition ciphers

The first basic type of cipher is the transposition cipher wherein the letters of the plaintext remain the same but are rearranged in a predetermined way (Janeczko, 2004). There are several types of transposition ciphers. Around 400 BCE, the Spartans and Greeks made use of a scytale cipher by writing a message on animal skin wrapped around a staff. While wrapped around the staff, the message was clear. However, once the animal skin was unwound, the message was transposed and appeared to be a string of random letters (Blackwood, 2009). During the Civil War, the rail fence cipher provided a way (that resembled a rail fence) to transpose letters in a message (Janeczko, 2004). In a route cipher, the letters of the plaintext message are written in a grid and then rearranged following a predetermined route on the grid (Janeczko, 2004). Although this method may not seem very secure, there is no record of any messages enciphered this way during the Civil War ever being deciphered (Blackwood, 2009).

Substitution Ciphers

In a substitution cipher the plaintext letters remain in order; other letters or symbols are simply substituted for each letter of the message (Janeczko, 2004). In a monoalphabetic cipher each plaintext letter is represented with the same ciphertext character throughout the message (Blackwood, 2009). The shift cipher, a monoalphabetic cipher, shifts the letters of the alphabet a given number of spaces to determine a letter's ciphertext substitution (Beissinger & Pless, 2006). Around 150 BCE, Polybius, a Greek historian, created the Polybius checkerboard which used a checkerboard form to replace each letter with a pair of numbers (Janeczko, 2004). The pigpen cipher uses symbols to represent each letter of the alphabet. This cipher was used by the Freemasons during the 1700s and was found in correspondence with a suspected Confederate spy during the Civil War (Janeczko, 2004). Other monoalphabetic systems pair letters randomly (Eskicioglu & Litwin, 2001). In the fifteenth century, Shihab al-Qalqashandi, an Egyptian cryptologist, used the concept of frequency analysis, the study of the relative frequencies of various letters in a given language, to determine the most likely letter represented by each symbol in the ciphertext in order to decipher texts that used monoalphabetic ciphers. After his discovery, monoalphabetic ciphers, used alone, were no longer secure (Blackwood, 2009). However, today, these simple substitution ciphers are used in combination with other operations to create secure ciphers (Eskicioglu, & Litwin, 2001).

Polyalphabetic ciphers

Once monoalphabetic ciphers were rendered obsolete, cryptographers began using polyalphabetic ciphers wherein each letter of the plaintext could be enciphered with multiple symbols or letters (Eskicioglu & Litwin, 2001). For example, in the same message, the letter e could be represented by B in one place, by Y in another place, and by 8 in yet another place. This action rendered frequency analysis obsolete

(Blackwood, 2009). Around 1466 in Florence, Italy, Leon Battista Alberti created the cipher disk, the first enciphering device that was both practical and secure (Blackwood, 2009). This revolutionary device paired one letter of plaintext with a letter of ciphertext for a few words and then changed the pairing in a way known only to the sender and receiver of the message (Blackwood, 2009). In 1499 Johannes Trithemius, a German monk, created a "crucial tool of modern cryptography, the tableau" (Blackwood, 2009, p. 35). In 1586, Blaise de Vigenére, a French scholar combined the ideas of Alberti and Trithemius and created The Vigenére Tableau. His tableau looked like Trithemius's (with a list of alphabets down the page with each alphabet shifted one space to the left) but included the use of a key word so that the alphabets were used in the order represented by the letters in the key (Blackwood, 2009). This cipher was considered unbreakable until 1854 when Cambridge mathematics professor Charles Babbage reasoned that if the key was short and the text was long the key length for a Vigenére cipher could be determined and the code broken. However, if the key is as long as or longer than the plaintext that is being enciphered, the cipher is still unbreakable as long as that key is only used once. (Beissinger & Pless, 2006).

Modern Cryptography

More recently, cryptographic methods use computer programing and mathematics with keys that involve complex algorithms (Sullivan, 2005). In 1976, the National Bureau of Standards adopted the Lucifer cipher as a standard to securely encrypt data. Even this cipher requires keys; however, it is not practical to safely deliver a key to senders and receivers of data on a large scale (Blackwood, 2009). In 1977, Ronal Rivest, Adi Shamir, and Leonard Adleman solved this problem with the RSA cipher. This cipher uses a public key that anyone can know to encrypt the data and a private key known only to the receiver to decrypt the data (Beissinger & Pless, 2006). This system uses a "two-key encryption system that is, for all practical purposes, unbreakable" (Blackwood, 2009, p. 154).

With the increased use of computers and technology, cryptography has expanded beyond its roots in encryption. It now addresses issues of data integrity and authenticity (K. Gopalakrishnan, personal communication, January 17, 2014). Ensuring data integrity assures senders and receivers of data that the data has not been changed by a third party while it was in transit (Kapoor, Pandya, & Sherif, 2011). Ensuring authenticity uses cryptographic protocols to ensure that the person who is believed to have sent the information actually did send the information. These protocols give people assurances that they are not dealing with an unauthorized party (Kapoor, Pandya, & Sherif, 2001).

Modern jobs in cryptography include cryptanalysts who analyze the security of cryptographic projects, cryptosystem designers who develop complex algorithms, cryptographic engineers who apply cryptography to solve human problems, and digital rights professionals who ensure the security of copyrighted digital material (Robyjose, 2011). People who study cryptography can also find employment as a university professor—an occupation that allows them to perform research concerning cryptography and teach others about the field.

<u>Summary</u>

Cryptography has evolved over millennia to address changing issues regarding secret information. Many of the methods used in the past—simple transposition and substitution to create codes and ciphers—are now obsolete. However, new practices in cryptography use more complicated mathematical formulas, large numbers for keys, and combinations of transpositions and substitutions to address the need for encryption, secrecy, data integrity, authentication, and user identification. However, cryptographers know that it is not easy to create a crypto-system that is really secure; eventually, a cryptanalyst will break most systems and a new one will need to be created (K. Gopalakrishnan, personal communication, January 17, 2014). Even with this knowledge, cryptographers realize that the meanings of some very old encoded messages remain concealed to this day (Blackwood, 2009). This knowledge keeps cryptographers looking for a new, perfect crypto-system that may, one day, be created.

References

Beissinger, J., & Pless, V. (2006). *The cryptoclub: Using mathematics to make and break secret codes*. Wellesley, MA: A.K. Peters/CRC Press.

Blackwood, G. (2009). *Mysterious messages: A history of codes and ciphers*. New York, New York: Dutton Children's Books.

Eskicioglu, A.M., Litwin, L. (2001). Cryptography, *Potentials, IEEE, 20*(1), 36-38. Doi: 10.1109/45.913211

Janeczko, P.B. (2004). *Top secret: A handbook of codes, ciphers, and secret writing*. Somerville, MA: Candlewick Press.

Kapoor, B., Pandya, P., & Sherif, J.S. (2011). Cryptography: A security pillar of privacy, integrity and authenticity of data communication. *Kybernetes, 40*(9/10), 1422-1439.

Romney, M. (1998). Cryptography. *Infotech Update, 7*(6), 9-10.

Robyjose (2011). *Cryptography as a Career Option.* Retrieved from http://www.studydiscussions.com/cryptography-as-a-career-option/

Sullivan, M. (2005). Cryptographer. *Science Teacher, 72*(8), 56.

CONNECTION TO THE THEME

What are INTERACTIONS? You and your partner need to operationalize your own definition of interactions.

Interaction is the action that occurs between or among multiple people or objects. Through this action, each of the people or objects has an influence or effect on the others. This effect is a two-way process; the effect is reciprocal. The interactions between people can serve to modify another's thoughts or opinions as well as their behavior or actions.

Communication is an example of interaction among people. Through communication, people can affect and influence others. With the increased use of technology, the world has become smaller and interactions among people who are further removed from each other has become commonplace. People can now sway influence over others virtually instantaneously from anywhere in the world. Interactions among people can have a powerful effect. The use of this instantaneous communication through social media has helped topple world governments. That is quite an influence!

How is the concept of INTERACTIONS depicted by your topic? Thoroughly explore how INTERACTIONS are depicted in your topic, especially in relation to your definition.

Cryptography is a tool that influences the interactions among people. It can increase or decrease interaction and encourage the interaction between code makers and code breakers. Cryptography is also involved in a direct interaction with computer technology. This interaction with technology also allows cryptography to interact with and have an effect on people as evidenced by people's behavior.

The use of cryptography can increase interaction among people or decrease interaction among people. The use of cryptography can increase interactions among people by providing a way to send sensitive information securely. Using codes and ciphers has enabled compatriots that are great distances away from one another to share plans and information without sharing the information with enemies. Without cryptography, this level of interaction would not be possible unless the parties involved were at the same location. In the computer age, the use of cryptography through public key encryption systems has increased the interactions among people even more. Now, not only do the people involved not have to be in the same place, they do not even have to know one another. Public key cryptography allows people to share sensitive information and provide services to one another even if they do not know each other and have not met to create a communication scheme. User identification schemes and authenticity protocols (modern applications of cryptography) also encourage interactions among people. With these systems, senders and receivers of information have confidence that the information they are receiving is from the appropriate person and that the data has not been changed in transit. In contrast, cryptography also provides a tool to decrease interaction among opposing forces. When a key is secret, people who do not know the key are unable to interact and influence those who know the key and vice versa. In this way, cryptography controls interactions among people; only people who know the key to the code or cipher can understand what is being said.

Cryptography also provides an avenue for the interaction between code makers (cryptographers) and code breakers (cryptanalysts). Cryptographers create codes and ciphers they believe to be secure. However, cryptanalysts are constantly trying to break the codes and ciphers that have been created. Eventually, the cryptanalyst will break the “secure” code, and the cryptographer will have to create a new, more complex, secure code. Faced with this new code, the cryptanalyst will have to create and use new techniques to break this new code or cipher. Eventually, the new code or cipher will be broken and the interaction between these two opposing forces will continue.

Cryptography interacts directly with computer technology. The creation of secure codes and ciphers allows computer technology to expand and provide more services and information to people. However, as computer technology becomes more powerful, cryptosystems used in the past become obsolete. Therefore, new cryptosystems and protocols must be created and the field of cryptography grows and expands to address new topics and concepts. These advances in cryptography again provide computer technology with the opportunity to share more information and grow even more powerful which causes this cycle of growth and adaptation to continue.

There is also an interaction between secure cryptosystems and people's behavior. A secure cryptosystem encourages people to participate in the world of e-commerce. However, when this security is breached (as in the recent hacking of Target and other retail stores) people's buying behavior changes and they are less likely to purchase items from stores with insecure encryption. This behavior encourages businesses to find more secure cryptosystems so that people will once again shop at their stores.

Through these situations, it is apparent that the use of cryptography has an effect on interactions among people and that cryptography interacts directly with technology. As the field of cryptography continues to grow and change, it will be interesting to see how much more influence the field will exert over interactions in the future.

TECHNOLOGY INTEGRATION

Technology has played a major role in the way cryptography has adapted and changed throughout history. It is, therefore, appropriate that technology play a major role in helping the students in our session, *Shhhhh...It's a Secret: Learning the Key to Cryptography*, learn how codes and ciphers work. In this unit, students will use a variety of technology tools and resources, including iPads, collaborative websites, informational online resources, virtual tools, practice exercises, and Skype.

The primary physical technology that will be used during this unit is the iPad. Students will use the iPads (connected to the internet) to ask questions, review information, collaborate with others, and view new content. They will also use the iPad's video capabilities to create their final product--an instructional video that will teach their "clients" the cryptosystem they create.

One collaborative website we will use is padlet.com. A padlet is an interactive "wall" onto which all participants can add information in a collaborative environment. Students will use padlets to create a group-wide list of pros and cons for each of the cryptosystems we discuss. Students will also be able to share their thoughts on which parts of each established code or cipher system they believe would be beneficial to use in their own cryptosystem. This forum will also allow students to view other students' ideas and learn from them. Students may even incorporate some other students' ideas into their cryptosystem in order to make it stronger and more secure. The final product is not a competition and this environment that encourages sharing will help students understand how technology tools can be used to expose students to a variety of ideas and opinions so that all the students can make the best product possible.

Throughout this unit, students will also make use of informational online resources. These resources include online videos, Prezis, and Slideshare slideshows. The online videos we will be using are located mostly on the websites YouTube.com and KhanAcademy.org. Prezis provide a tool for the creation of presentations that do not flow in a linear manner. Typically, the design of the presentation itself helps enhance the information being presented. Slideshare is a slide hosting resource that allows people to upload and share their slide presentations with others. These informational resources will serve two purposes. First, they will present content to the students about each of the cryptosystems we will be discussing. Students will then be able to apply that content to decrypt and encrypt information. Secondly, the resources will provide models for the instruction that the students will be creating for their final product. The instructional videos used will be especially appropriate since that is the type of instruction the students will be creating for their product. However, the use of Prezis and Slideshare slideshows will demonstrate other options for instruction that students can use in the future.

Students will also have the opportunity to make use of virtual tools during our unit. The students will use a virtual cipher wheel (http://inventwithpython.com/cipherwheel/), a virtual Vigenére tableau (http://www.mathman.gr/component/content/article/10/639-cryptography-Vigenére-cipher.html), and a Vigenére cipher tool (https://www.khanacademy.org/math/applied-math/cryptography/ciphers/e/Vigenére_cipher_encryption). On day three, our focus will be on breaking ciphers. During this lesson, students will be able to use an online tool (http://rumkin.com/tools/cipher/frequency.php) that counts the number of times each letter appears in a given text. This tool will do the tedious work of gathering the data the students will use to perform a frequency analysis on the letters in the text and allow students to get to the active cipher-breaking part of the lesson more quickly. This tool will also help students understand how cryptanalysts use the technology tools at their disposal in order to break ciphers while demonstrating the effect that improved technology has had on the types of ciphers that are being created now. Finally, students will use Quizlet.com, a student directed online learning tool that allows students to learn new vocabulary through a variety of activities and games. Using this tool will help students understand the vocabulary being used in our unit.

The final technology tool our sessions will use is Skype--an online product that provides a video conferencing function. At the beginning of the week, our students will be given a challenge to create a secure cryptosystem for another group of students. This challenge was also given to a group of students at D. F. Walker Elementary School. On Thursday, that group of students (who have already created their own cryptosystem) will Skype with our camp students, and all the students will discuss the established cryptosystems and their ideas about the new cryptosystems they are creating or have created. In this way, the camp students will be interacting with other students who have a common goal, and they will be learning more about the power of technology to enable people to work together to solve a problem. Our camp students can then incorporate new information and ideas (as they deem it appropriate) into the creation of their new cryptosystem.

Technology plays a vital role in the world today, and it is only appropriate that we make use of these tools to enhance the learning of our students. The variety of tools that we will be using will provide students with the opportunity to learn the content for the week, experience how technology has made established ciphers less secure, view applications that can be used for this camp week and beyond, and demonstrate their understanding of the content through comments and their final product. These uses of technology will definitely enrich our unit!

CONTENT OUTLINE

1. Description/Definition
   A. The art of writing messages with hidden meaning
   B. From the Greek for "hidden, secret" and "writing" or "study"
   C. Practice and study of secure communication in the presence of a third party
2. Vocabulary/Terminology
   A. Plaintext
      1. Text as it is ordinarily written
      2. Information a sender wishes to transmit to a receiver
   B. Ciphertext
      1. Enciphered or encoded text
      2. Secure form of the text as it is transmitted in order to protect it from third parties
3. Historical examples and uses of cryptography
   A. Military
      1. Navajo code talkers in World War II
      2. Route ciphers used in the Civil War--there is no record of these being deciphered
   B. Political
      1. Code book used by James Madison and Thomas Jefferson around 1793
      2. Julius Caesar used a shift cipher for communication that shifted the letters of the alphabet 3 places to the left.
4. Codes
   A. Control interaction among people since only those who know the key can understand and participate in the communication
   B. A type of secret communication which replaces entire words in a given text with other words, numbers, or symbols
   C. Non-secret codes
      1. Zip codes
      2. Area codes
   D. Secret codes
      1. Dictionary codes
         a) Changes each word to a multi-digit number
         b) The multi-digit number includes the page number, the column number, and the line number on which the word is located in the dictionary.
         c) The message sender and receiver must use the same version of the dictionary.
      2. Code book codes
         a) Can be created by anyone
         b) A code book takes a long time to create since it must contain all of the words that a person sending a message might need

c) Encoding book lists plaintext words systematically (perhaps alphabetically) with their ciphertext equivalent beside it

d) There can be a second decoding book that lists the ciphertext words, symbols, or numbers in a systematic way with the plaintext equivalent beside it to make decoding easier

E. Spoken codes

1. Navajo code--Code Talkers

a) Used during WWII by the allies

b) Code was never broken

2. Pig Latin

3. Turkish Irish

F. Advantages of using codes

1. It is easy to find a word to encode it or a symbol to decode a message when the words are listed in a systematic way in a code book.

2. There are fewer individual symbols to decrypt since the entire word is decrypted at the same time.

G. Disadvantages of using codes

1. If the code book is lost or stolen, the code is no longer secure.

2. Creating a new code book is very time consuming.

3. Code books are cumbersome to carry around and too long to memorize.

5. Ciphers

A. Control interactions among people since only those who know the key can understand and participate in the communication

B. A type of secret writing which replaces each letter in the text with a different letter, number, or symbol

C. Vocabulary

1. Algorithm

a) Mathematical formula for converting text

b) Well defined steps followed to encipher text

2. Key

a) Number that is used in the algorithm

b) Word that is used as a guide to encipher and decipher text

D. Transposition Ciphers

1. The letters in the plaintext are not changed

2. The letters of the plaintext are rearranged to hide the meaning of the enciphered text

3. Examples

a) Rail fence cipher

(1) Named because the placement of the letters during the transposition resemble a rail fence

(2) Used during the Civil War

b) Route cipher

- (1) Letters of the text are written in a grid and rearranged following a predetermined route
- (2) No evidence exists that this type of cipher was broken during the Civil War although it was used often

E. Advantages

- 1. Requires a long time for someone to break the cipher by hand because there are a lot of different combinations of letter positions possible
- 2. The ciphertext which results from the transposition cipher makes no sense.

F. Disadvantages

- 1. Susceptible to deciphering by computer
- 2. Not highly secure because the letters do not change

6. Substitution Ciphers

- A. The letters in the plaintext remain in the same order but other letters, numbers, or symbols replace them to form the ciphertext
- B. Monoalphabetic Ciphers
  - 1. Uses the same letter, number, or symbol to represent a given letter throughout the ciphertext
  - 2. Examples
    - a) Shift Cipher
      - (1) Caesar cipher is an example used by Julius Caesar
      - (2) Shifts each letter of the alphabet a given number of spaces to determine the letter that would represent it in the ciphertext
    - b) Pigpen cipher
      - (1) Named because some thought the form of the cipher symbols resembled a pig pen
      - (2) Believed to have been used by the Free Masons
      - (3) Uses symbols to represent each letter of the alphabet
  - 3. Advantages and Disadvantages
    - a) Advantages
      - (1) Easy to encipher and decipher text
      - (2) There are tools available to help encipher and decipher text
      - (3) Cipher key is easy to remember
    - b) Disadvantages
      - (1) Susceptible to frequency analysis
      - (2) No longer secure when used alone
- C. Polyalphabetic ciphers
  - 1. Uses different ciphertext characters to represent the same plaintext character in the same enciphered message
  - 2. Examples
    - a) Alberti Cipher
      - (1) Created in 1466 in Florence, Italy by Leon Battista Alberti

(2) Uses a cipher wheel

(a) Two concentric circles with a common center and the smaller one on top of the larger one

(b) Twenty-six sections go around the circumference of each circle--one for each letter of the alphabet

(c) The letters of the alphabet are written in order around the edge of the surface of each circle

(d) The circles are rotated to line the plaintext letters (on the outer circle) with their ciphertext letters (on the inner circle)

(3) The letter that aligns with the letter a on the cipher wheel is indicated in the cipher by a capital letter

(4) After a few words are enciphered, the wheel is rotated to pair the plaintext letters and ciphertext letters differently

b) Vigenére Cipher

(1) Created in 1586 by Blaise de Vigenére who combined the works of Leon Battista Alberti and Johannes Trithemius

(2) Uses a tableau (like Trithemius’s) which is a list of 26 alphabets down the page with each successive alphabet’s letters shifted one place to the left

(3) Uses a key word to indicate the order in which the alphabets will be used to encipher text

3. Advantages

a) More difficult to break than monoalphabetic ciphers because if a single ciphertext letter is known it cannot be substituted throughout the ciphertext because it may represent different letters at different times

b) Not susceptible to frequency analysis

4. Disadvantages

a) If the key is short and the text is long, the length of the key may be determined and the cipher broken

b) Using the key again makes it less secure

5. One-time pad

a) Uses an infinite number of unique keys that are as long as or longer than the plaintext so that there are no repeating patterns in the ciphertext

b) Advantages

(1) Theoretically unbreakable

(2) Most secure cipher system

c) Disadvantages

(1) Key must be as long or longer than the text that is being encrypted

(2) Key can only be used once

(3) If the key is accidentally used more than once, data can be gathered and frequency analysis is possible

(4) Unlimited number of keys are necessary

7. Cryptanalysis
   A. The art of figuring out the secret meanings of messages
   B. The process of analyzing encrypted messages for patterns in order to determine the key and "break" a cryptosystem
   C. Creates a competition or "game" between cryptographers and cryptanalysts
   D. Interacts with cryptography in a way that causes a constant cycle of change
      1. A cryptosystem is broken using cryptanalysis
      2. Cryptographers create a stronger and more secure cryptosystem
      3. Cryptanalysts use more advanced techniques to break the new cryptosystem and the cycle continues
   E. Frequency analysis
      1. First used by the fifteenth century Egyptian cryptologist, Shihab al-Qalqashandi
      2. Involves the analysis of words or symbols representing words to find patterns in codes
      3. Involves the analysis of the number of times each symbol or letter appears in a given example of ciphertext in monoalphabetic ciphers
      4. Cannot be applied to short examples of codes and ciphers since there will not be enough data
      5. Can be used on data collected from multiple examples of short ciphertext if the key is used multiple times
      6. Frequencies of letters vary based on the language of the plaintext used in the cipher
   F. Polyalphabetic Ciphers
      1. In 1854, Cambridge mathematics professor Charles Babbage reasoned that if the key was short and the text was long the key length could be determined for a Vigenére cipher and the cipher could be broken
      2. Involves the analysis of text to find repeating patterns in the letters, symbols, and numbers in the ciphertext
      3. The distances between these repeating patterns helps determine the key length
      4. Once the key length is known, the ciphertext becomes multiple examples of monoalphabetic ciphers that are susceptible to frequency analysis.
   G. "Hacking" techniques
      1. Determine a vulnerability in a system so that enough data can be gathered to determine the key
      2. BEAST Exploit to crack web encryption
         a) Uses suspicious links or malicious websites to infect a computer

b) Uses malicious program to monitor data exchanged between the computer and secure websites

c) Program inserts blocks of plaintext and attempts to decrypt those blocks by guessing the encryption key

d) Program gathers enough data to correctly find the key and uses it to reverse engineer the key and decrypt confidential data stored on the computer

8. Cryptography's interaction with Computer Technology

A. Creation of secure codes and ciphers allows computer technology to expand and provide more services and information to people

B. As computer technology becomes more powerful, cryptosystems used in the past become obsolete

C. New cryptosystems and protocols must be created and the field of cryptography grows and expands to address new topics and concepts and the cycle continues

9. Modern Applications

A. RSA cipher

1. Created in 1977 by Ronal Rivest, Adi Shamir, and Leonard Adleman

2. Asymmetric cipher where two keys are used--an encryption key and a decryption key

3. Allows people who are unknown to each other to communicate securely

4. Makes use of prime factors of very large numbers so that it takes a lot of time to break the cipher even using the combined power of many computers--this makes it unbreakable in a practical sense

B. Data integrity

1. Makes sure that the data being sent has not been changed by a third party while it was in transit

2. Encourages interactions among people because the senders and receivers know that the data has not been changed or tampered with

C. Data authentication

1. Determines whether the supposed sender of the data actually sent the data

2. Determines that no one else is pretending to be the person who supposedly sent the message

3. Uses a digital signature that is confirmed by a third party

4. Encourages interactions among people because a receiver has assurances that the alleged sender actually sent the communication

10. Jobs involving cryptography

A. Cryptanalysts

1. Analyze the security of cryptographic projects

2. Break cryptosystems

B. Cryptosystem designers

1. Create complex algorithms called cryptographic systems to use to encipher information
2. Work for technology companies and governments

C. Cryptographic engineers
1. Use cryptography to solve human problems
2. Typically address issues of data confidentiality, data integrity, and the authentication of people and devices

D. Digital rights professionals
1. Ensure the security of copyrighted digital materials
2. Use cryptographic keys to "scramble" information so that it cannot be illegally copied

E. University professors
1. Perform research in cryptography
2. Teach others about cryptography

LESSON #1
Establishing the Mission

I. DEFINE OBJECTIVES AND CONTENT	
LESSON OBJECTIVE	The learner will use at least two different established cryptosystems to encrypt and decrypt information and will explain at least two positive aspects and two negative aspects of each of those systems.
POINT TO PONDER	Secrets are necessary for a stable society.
ESSENTIAL QUESTION	How do secrets affect our **INTERACTION** with others?

CONTENT Outline the content you will teach in this lesson.	1. Description/Definition A. The art of writing messages with hidden meaning B. From the Greek for "hidden, secret" and "writing" or "study" C. Practice and study of secure communication in the presence of a third party 2. Vocabulary/Terminology A. Plaintext 1. Text as it is ordinarily written 2. Information a sender wishes to transmit to a receiver B. Ciphertext 1. Enciphered or encoded text 2. Secure form of the text as it is transmitted in order to protect it from third parties 3. Historical examples and uses of cryptography A. Military 1. Navajo code talkers in World War II 2. Route ciphers used in the Civil War--there is no record of these being deciphered B. Political 1. Code book used by James Madison and Thomas Jefferson around 1793 2. Julius Caesar used a shift cipher for communication that shifted the letters of the alphabet 3 places to the left. 4. Codes A. Control interaction among people since only those who know the key can understand and participate in the communication B. A type of secret communication which replaces entire words in a given text with other words, numbers, or symbols C. Non-secret codes 1. Zip codes 2. Area codes D. Secret codes 1. Dictionary codes a) Changes each word to a multi-digit number b) The multi-digit number includes the page number, the column number, and the line number on which the word is located in the dictionary.

c) The message sender and receiver must use the same version of the dictionary.

2. Code book codes

a) Can be created by anyone

b) A code book takes a long time to create since it must contain all of the words that a person sending a message might need

c) Encoding book lists plaintext words systematically (perhaps alphabetically) with their ciphertext equivalent beside it

d) There can be a second decoding book that lists the ciphertext words, symbols, or numbers in a systematic way with the plaintext equivalent beside it to make decoding easier

E. Advantages of using codes

1. It is easy to find a word to encode it or a symbol to decode a message when the words are listed in a systematic way in a code book.

2. There are fewer individual symbols to decrypt since the entire word is decrypted at the same time.

F. Disadvantages of using codes

1. If the code book is lost or stolen, the code is no longer secure.

2. Creating a new code book is very time consuming.

3. Code books are cumbersome to carry around and too long to memorize.

5. Ciphers

A. Control interactions among people since only those who know the key can understand and participate in the communication

B. A type of secret writing which replaces each letter in the text with a different letter, number, or symbol

C. Vocabulary

1. Algorithm

a) Mathematical formula for converting text

b) Well defined steps followed to encipher text

2. Key

a) Number that is used in the algorithm

b) Word that is used as a guide to encipher and decipher text

6. Substitution Ciphers

A. The letters in the plaintext remain in the same order but other letters, numbers, or symbols replace them to form the ciphertext

B. Monoalphabetic Ciphers

1. Uses the same letter, number, or symbol to represent a given letter throughout the ciphertext

2. Examples

a) Shift Cipher

(1) Caesar cipher is an example used by Julius Caesar

(2) Shifts each letter of the alphabet a given number of spaces to determine the letter that would represent it in the ciphertext

b) Pigpen cipher

(1) Named because some thought the form of the cipher symbols resembled a pig pen

(2) Believed to have been used by the Free Masons

(3) Uses symbols to represent each letter of the alphabet

3. Advantages and Disadvantages

a) Advantages

(1) Easy to encipher and decipher text

(2) There are tools available to help encipher and decipher text

(3) Cipher key is easy to remember

b) Disadvantages

(1) Susceptible to frequency analysis

(2) No longer secure when used alone

II. PRE-PLANNING

What will students UNDERSTAND as a result of this lesson? How does this connect to the Essential Question?	1. Students will understand that codes and ciphers were originally used to keep secrets for military and political purposes. This understanding will help students determine and discuss ways that secrets (and the use of cryptography) have affected governments through their military and political purposes. This will show how secrets have affected **INTERACTIONS** among governments and peoples. 2. Students will understand how to use at least one established code system and at least one monoalphabetic cipher system. This understanding will help students identify how these code and cipher systems, as well as the secrets that are necessary to keep in order to use the systems and the secrets created with the systems, affect the **INTERACTIONS** between and among people. Through their experiences using the code and cipher systems, they will be able to make connections to how **INTERACTIONS** would be affected if someone did not understand the code or cipher key. They will also be able to explain the differences in the **INTERACTIONS** that take place among people who all know the code or cipher key being used and the **INTERACTIONS** that take place among group members when some know the code or cipher key and others do not.
What will students be able to DO as a result of this lesson?	Students will be able to decode a message and encode a message using at least one established code system. Students will be able to decipher a message and encipher a message using at least one monoalphabetic cipher system. Students will be able to list and explain at least 2 positive aspects and 2 negative aspects of each of the cryptosystems they experience.

III. PLANNING	
HOOK Describe how you will grab students' attention at the beginning of the lesson. BE CREATIVE.	TIME: 5 minutes Nancy will have a group of her students from her school create a video that we will show the students as our hook. In this video, a group of students is competing in a "Survivor game" where they have to find hidden objects before another team does. However, one of the teams manages to get on the same walkie-talkie frequency as the other team. The team then realizes that they need to use some type of secret communication and asks for help. After viewing the video, Nancy and Carol will explain that we received this video asking for help and have decided to have our sessions help this group of students. We will explain that, since the creators of the competition did not agree with the Grizzle's behavior, they stopped the competition and have given both teams extra time to prepare. By the end of this week, if we accept the challenge, we should have several cryptosystems created to teach to the Blackhawks so that they can choose one to use when the competition resumes. Our challenge will be to create the most appropriate cryptosystem for the group. (See attached script and https://docs.google.com/file/d/0B4u2Cf2z0XcmLVZ0SExyTlRKb3c/edit) This mission sets the students up for their final product for the week. For this product, students will work in pairs (or a group of three depending on the number of students in the session) to create a new, secure cryptosystem, explain why they believe their system is secure, and create an instructional video to send to the group asking for help in order to teach them the new cryptosystem. We will end by discussing how using a cryptosystem would affect the **INTERACTIONS** among the teammates asking for help as well as among the different teams. How would these "secrets" affect their **INTERACTIONS** (essential question reference)?
INSTRUCTION Explain Step-by-step what you will do in this lesson. Be explicit about ties to Points to Ponder, Essential Question,	TIME: 60 minutes 1. As students enter the classroom they will receive a card that contains a number and a letter. The students whose numbers match will be station partners for the week. Students whose letters match will be cryptosystem creation partners for the week. The cards will also indicate the order in which each set of station partners will complete the stations. (See attached card forms.) 2. Students will brainstorm why they think people would need codes and ciphers. We will list all ideas shared on the SmartBoard. Ideas should include for military and political purposes. (We will guide students to makes sure these points are mentioned if necessary.) We will specifically mention the code book used by James Madison and Thomas Jefferson, the

and Interactions here. Include ALL support and teaching materials with your unit.	Caesar cipher used by Julius Caesar, the Navajo code talkers of WWII, and the route ciphers used during the Civil War. We will pose the point to ponder to students and get their initial thoughts. (If necessary we, with the help of the students, will define stable to make sure everyone understands.) We will also discuss how these political and military secrets affect **INTERACTIONS** among governments and peoples.(3 minutes) 3. As a group, we will define cryptography. We will make sure, as the group discusses cryptography's meaning, that the information located on the content outline is included. 4. Have students practice learning the following vocabulary words on iPads using the app Quizlet: monoalphabetic cipher, ciphertext, plaintext, algorithm, key, substitution cipher, encode, decode, encipher, and decipher. After practicing the words using Quizlet, each student will be shown how to use the Frayer model to learn new vocabulary words with the examples of code and cipher. (see attached) Students will be instructed to complete a Frayer sheet at each of their stations (either Dictionary Code, Code Book, Shift Cipher or Pigpen Cipher) to teach their teammates about their station code/cipher. (10 minutes) 5. Pass out crypto-journals to students (see attached—will be printed on front and back of papers and folded into a booklet). These journals will be used throughout the week for note-taking, working out codes and ciphers, completing assessments, and planning the final products. 6. Explain to students that they will be learning and using at least one code system at least one cipher system today. Explain the way the stations will work and where on their card they will find their station completion order. (2 minutes) 7. Students will attend their first assigned station with their station partner and rotate to a new one as they finish. The stations below will run simultaneously. Each student should complete at least two stations. Cryptosystem creation teams will complete different stations so that they can share information with one another and incorporate all ideas into their final product. As students work in each of the stations, the teachers will be available to discuss their work, answer questions, and guide informal discussions with each group that will help them see possible positive aspects and negative aspects of each system as well as how these systems that create secrets affect the **INTERACTIONS** among people and how using systems such as these would affect a society. Would they help keep the society stable? (We will make sure the students make connections about how the **INTERACTIONS** between groups who all know the key to the secrets differ from the **INTERACTIONS** among

groups where some know the key and some do not.) These connections are to our point to ponder, essential question, and **INTERACTIONS** theme. During the informal discussions in the stations, the instructors will make sure to guide students to understand the advantages and disadvantages of codes and monoalphabetic ciphers that are listed in the content outline.

Station 1 (approx. 20 min)

Dictionary Code

1. Students will view the dictionary code Slideshare on their iPads located at: http://www.slideshare.net/nancyheiniger/dictionary-code-32397273
2. Students will then use the dictionaries and coded message cards (see attached) provided to practice this method.
3. Students will use the dictionary code to decode a clue to the identity of a hidden object in our room. Then, students will use the dictionary code to encode their guess as to the identification of the hidden object. (see attached)
4. Students will use the Frayer model to explain the definition of Dictionary Code with their partner.
5. In their crypto-journal, students will write at least 2 positive aspects of the dictionary code and at least 2 negative aspects of the dictionary code.
6. A mini display board will be provided at this station to reinforce the information provided to them on the slideshare. (see attached)

Object identity: spyglasses
Clue: one eyed telescope

Station 2 (approx. 20 min)

Code book code

1. Students will view a short Prezi on their iPads on how this code method works located at: http://prezi.com/xetktgfw3l0u/code-book/
2. Students will use the code book and coded message cards (see attached) provided at this station to practice this method.
3. Students will use the codes provided in the code book to decode a clue to the identity of a hidden object in our room. Students will then use the codes provided in the code book to encode their guess as to the identification of the hidden object.(see attached)
4. Students will use the Frayer model to explain the definition of Code book code with their partner.
5. In their crypto-journal, students will write at least 2 positive aspects of the code book code and at least 2 negative aspects of the code book code.

6. A mini display board will be provided at this station to reinforce the information provided to them on the Prezi.
   Object identity: spyglasses
   Clue: The better to see you with

Station 3 (approx. 20 min)

Shift Cipher

1. Students will view the video located at https://docs.google.com/file/d/0B13_mZTJNpttNC1OSHFGWFlsT1E/edit?pli=1 to learn about the shift cipher. Then they can view the video at the following link if they want more information http://www.youtube.com/watch?v=GpQeOT0Mqys&feature=youtu.be They will view from the beginning of the video to the 4:40 mark on the video. Students will be told that they can view the rest of the video at home if they are interested and have permission.
2. Students will use the tool located at cryptoclub.math.uic.edu/shiftcipher/shiftcipher.htm or the physical cipher wheel provided in the station to decipher the texts located on the self-checking cards (see attached)
3. Students will use the cipher wheel provided at the station or the virtual cipher wheel located at http://inventwithpython.com/cipherwheel/ or cryptoclub.math.uic.edu/shiftcipher/shiftcipher.htm to decipher a clue to the location of a hidden object. They will then use the shift cipher tool they have chosen to encipher their guess as to the location of the hidden object.
4. Students will use the Frayer model to explain the definition of shift cipher to their partner.
5. In their crypto-journal, students will write at least 2 positive aspects of the shift cipher and 2 negative aspects of the shift cipher.
6. A display board will be in the station to reinforce the information presented about this cipher and to provide additional information to the students (see attached forms).

Station 4 (approx. 20 min)

Pigpen Cipher

1. Students will view the Prezi located at http://prezi.com/a-nyaz1-lem9/pigpen-cipher/ and the video located at https://drive.google.com/file/d/0B8_Iy2-ce3qlNjdfQnBFZDlhTUU/edit?usp=sharing
2. Students will use the supplied pigpen cipher form (see attached) to complete the self-checking pig riddles (also attached).
3. Students will use the supplied pigpen cipher form to decipher a clue to the location of a hidden object in our room. They

	will then use the Pigpen Cipher form to encipher their guess as to the location of the hidden object. 4. Students will use the Frayer model to explain the definition of pigpen cipher to their partner, 5. In their crypto-journal, students will write at least 2 positive aspects and 2 negative aspects of the pigpen cipher. 6. A display board will be in the station to reinforce the information presented about this cipher and to provide additional information to students (see attached forms). 8. After 40 minutes, we will reassemble as a group and discuss the students' experiences with the codes and ciphers. As a class, we will discuss what students found to be easy or hard at each station. We will also discuss their thoughts about the codes and ciphers. We will provide an opportunity for students to share how these codes and ciphers and the secrets that they are used to hide affect **INTERACTIONS**, and we will revisit the idea of the need for secrets to create a stable society. 9. Students will meet with their cryptosystem partner and discuss the different systems they experienced at the stations. With their partner, students will brainstorm what they saw as important aspects that should be considered in creating a good code or cipher. We will share these ideas as a class. Possible suggestions may include: it should be easy to remember, it should be easy to use, it should be difficult to figure out, it should be convenient to carry the key with you or memorize it, etc. The students will record what they believe to be the most important aspects to consider in their crypto-journal so they will consider these aspects as they create their own cryptosystem.
ASSESSMENT (Performance Task) What will the students DO to demonstrate that they have mastered the content? Be specific and include actual assessment	TIME: 5 minutes At each station, the students will decode or decipher the message at that station and encode or encipher their guess as to what and where the hidden object for the day is. In their crypto-journal, students will write down at least two positive aspects and two negative aspects of each of the cryptosystems they experienced today. At the end of class, students will have an opportunity to add the positive and negative aspects they noted about each of the cryptosystems they experienced today to our class padlet for today.

with unit materials.	

DOES THE ASSESSMENT ALLOW YOU TO DETERMINE WHETHER OR NOT THE STUDENTS HAVE MET YOUR STATED LESSON OBJECTIVE?   [✓ YES] OR NO

ASSESSMENT AND INSTRUCTIONAL MATERIALS
Insert ALL materials here including Assessments and Instructional Materials.
Explicitly LIST any additional files for this lesson. Be sure that ALL materials have been submitted for this lesson.

Files and links needed for this lesson:
(All of these links are located on our session website and, whenever possible, the videos or other instruction are embedded on the website. They are also listed in the lesson plan at the appropriate places.)

Dictionary Code Slideshow
http://www.slideshare.net/nancyheiniger/dictionary-code-32397273

Code Book Prezi
http://prezi.com/xetktgfw3l0u/code-book/#

Shift Cipher Video
http://www.youtube.com/watch?v=GpQeOT0Mqys&feature=youtu.be

Interactive Cipher Wheel
http://cryptoclub.math.uic.edu/shiftcipher/shiftcipher.htm

Pigpen Cipher Prezi
http://prezi.com/a-nyaz1-lem9/pigpen-cipher/

Pigpen Cipher Video
https://docs.google.com/file/d/0B8_Iy2-ce3qlNjdfQnBFZDlhTUU/edit?pli=1

Padlet for Day 1
http://padlet.com/wall/i4r42zpqn8

Attachments for Day 1:

Colored cards for grouping students as they enter the session on Day 1

1A Station order 1, 3, 2, 4	1B Station order 1, 3, 2, 4
1C Station order 1, 3, 2, 4	1D Station order 1, 3, 2, 4
1E Station order 1, 3, 2, 4	1F Station order 1, 3, 2, 4
2A Station order 4, 2, 1, 3	2B Station order 4, 2, 1, 3
2C Station order 4, 2, 1, 3	2D Station order 4, 2, 1, 3

Colored cards for grouping students as they enter the session on Day 1

2E Station order 4, 2, 1, 3	2F Station order 4, 2, 1, 3
3A Station order 3, 1, 4, 2	3B Station order 3, 1, 4, 2
3C Station order 3, 1, 4, 2	3D Station order 3, 1, 4, 2
3E Station order 3, 1, 4, 2	3F Station order 3, 1, 4, 2
4A Station order 2, 4, 3, 1	4B Station order 2, 4, 3, 1

Colored cards for grouping students as they enter the session on Day 1

4C Station order 2, 4, 3, 1	4D Station order 2, 4, 3, 1
4E Station order 2, 4, 3, 1	4F Station order 2, 4, 3, 1
5A Station order 3, 1, 4, 2	5B Station order 3, 1, 4, 2
5C Station order 3, 1, 4, 2	5D Station order 3, 1, 4, 2
5E Station order 3, 1, 4, 2	5F Station order 3, 1, 4, 2

The Survival Games Script

Written by: Jacob Twiddy & Jacob Brooks

Editor: Mrs. Heiniger

Scene*: (In the woods with ribbon that says, "Welcome" strung between 2 trees*)

Characters: Tom Knapp – host of Survivor games; Blackhawks team members: Robert, Ben, Frank, Jacob, Grizzlies #1, 2, 3

Tom Knapp: Welcome to the 6th annual Survival Games. We know you have come far to participate in this event. Let's go over the rules. Rule#1: To win the Survival Games you must find 3 objects hidden around the woods and bring them to a teepee hidden in the woods. Rule#2: The first team to bring their three objects to the teepee wins the Survival Games and $50,000! I am going to give each team a card with the items they need to collect on it. There are 2 of each item in the same place that you need to collect, so each team has a chance of winning. If you pull out both of the same objects your team will be disqualified. When you find an object, tag it with your team name so the opposing team doesn't steal it. I wish you all good luck. (*cuts ribbon) BEGIN!

Frank: Go! (*Both teams run and then split up.)*

camera on Blackhawks, Blackhawks run through woods, Blackhawks stop

Scene: Woods

Jacob: STOP!

Robert: What?

Jacob: First, we need to know what we are looking for

Frank removes card

Frank: Peacock Feather? Quartz Chunk? Leopard Fur? What the heck?

Robert: We are going to have to split up into 3 groups to find all of these objects quicker.

Frank: How will we communicate?

Ben: We can use our walkie-talkies.

Frank: Okay

Robert: I'll go with Fred.

Ben: I'll go with Frank.

Jacob: I'll go alone.

Ben: Let's get moving!

Frank: O.K. let's go

Blackhawks split up

Fade out

fade in to Grizzlies

Grizzly#1: We haven't found anything

Grizzly#2 Duh, it would help if we pulled out our list

Grizzly#3 *pulls out list*

Grizzly#1: Quartz Chunk? Peacock Feather? Leopard Fur?

Grizzly#2: HOW ARE WE SUPPOSED TO FIND A QUARTZ CHUNK IN THE MIDDLE OF A FOREST!!!

Grizzly#3: They are hidden in the woods, you fool; we don't actually have to mine quartz.

Grizzly#1: Let's split up to find it faster.

Grizzly#2: We can use our walkie-talkies to talk

Grizzlies split into 2 groups

Fade out

Fade into Jacob

Jacob: I think I found something

Reaches into a hollow in a giant oak tree

Jacob: The Block of Quartz!

fade out

Fade into Grizzlies group 1

Grizzly#1: We should ask the other group if they have found anything

Jacob on walkie-talkie I found the block of quartz.

Robert on walkie-talkie Great, where is it

Jacob on walkie-talkie In a hollow in a g----

Grizzlies mumbling excitedly in background

Jacob on walkie-talkie What

silence

Jacob: The Grizzlies!!!!!

Jacob: THEY ARE ON OUR CHANNEL

Jacob: I've got to make a code to tell them the location of my spot, but how? We need help from expert code writers - anyone out there to help us?

(Note - when my two students from D. F. Walker Elementary School Skype the Pitt County Group, they are going to tell them that they intercepted this message and were trying to work on a code but needed more help. They heard the Pitt County Group was working on the code also and wanted to know what they came up with.)

Frayer Model

DEFINITION IN YOUR OWN WORDS

DOES NOT INVOLVE MEANING –
MECHANICAL OPERATION (ALGORITHM)
PERFORMED ON INDIVIDUAL OR
CHUNKS OF LETTERS
DOES NOT REQUIRE CODEBOOK
JUST FOLLOW THE DIRECTIONS

CHARACTERISTICS/ILLUSTRATION

A	C	A
T	M	E
O	W	S

ATOCMWAES

SOLVE BY READING
HORIZONTALLY ACROSS THE
GRID

CIPHER

EXAMPLES/MODELS - 3

RAIL FENCE CIPHER
ROUTE TRANSPOSITION CIPHER
ALBERTI CIPHER
MORSE CODE

NON-EXAMPLES - 3

TEXTING CODE
DICTIONARY CODE

Frayer Model

DEFINITION IN YOUR OWN WORDS	**CHARACTERISTICS/ILLUSTRATION**
MAPPING FROM SOME MEANINGFUL UNIT (SENTENCE, WORD OR PHRASE) INTO SOMETHING ELSE (USUALLY SHORTER GROUPS OF SYMBOLS)	BFF – BEST FRIENDS FOREVER TXT - TEXT

CODE

EXAMPLES/MODELS - 3	NON-EXAMPLES - 3
TEXTING CODE DICTIONARY CODE	RAIL FENCE CIPHER ROUTE TRANSPOSITION CIPHER ALBERTI CIPHER MORSE CODE

My Crypto-Journal

Name: ______________________

Session Time: ________________

Day 1

Plan your video instruction here and on the back of this page.

First Station Name: ______________

Practice Area for First Station:

First Cryptosystem
Positive Aspects (at least 2):

Negative Aspects (at least 2):

Explain how your cryptosystem works.

Provide at least one example using your cryptosystem.

Notes from Day 1/Station 1

Day 1

Second Station Name: ___________

Practice Area for Second Station:

Second Cryptosystem
Positive Aspects (at least 2):

Negative Aspects (at least 2):

Cryptosystem Creation Form

What is the name of your new cryptosystem?

Did you use any aspects of the cryptosystems we learned this week? If so, which one(s)?

List at least 3 aspects of your cryptosystem that you think makes it secure (or at least secure enough for the purposes of this project).

1.

2.

3.

More Notes to help create your cryptosystem

Notes from Day 1/Station 2

Notes from Day 1 to help with Cryptosystem Creation

General notes to help with Cryptosystem creation

Day 4 assessment:

Explain at least one way that your cryptosystem has been improved through collaboration with others.

Day 2

First Station Name: ______________

Practice Area for First Station:

First Cryptosystem
Positive Aspects (at least 2):

Negative Aspects (at least 2):

Notes from Day2/Station 1

Day 4

Notes to help with Cryptosystem creation

Day 4

Notes from Skype conversation

Day 2

Second Station Name: ___________

Practice Area for Second Station:

Second Cryptosystem
Positive Aspects (at least 2):

Negative Aspects (at least 2):

Notes from Day 2/Station 2

Day 4

Notes during Modern Cryptography Application activity

Use the space below to write anything that might help with planning and presenting this activity.

Day 3

Notes to help with Cryptosystem creation project

Notes from Day 2

Day 3
Notes

Day 3
More Notes

Dictionary Code Station

- Pages for Display on the Dictionary Code Board

1. Definition
2. Example of dictionary code and how to decode it
3. Picture of a dictionary code
4. Did you know? Facts about Dictionary Codes
5. Student observation page

- Dictionary code form

- Self-checking cards for practice with the Dictionary code

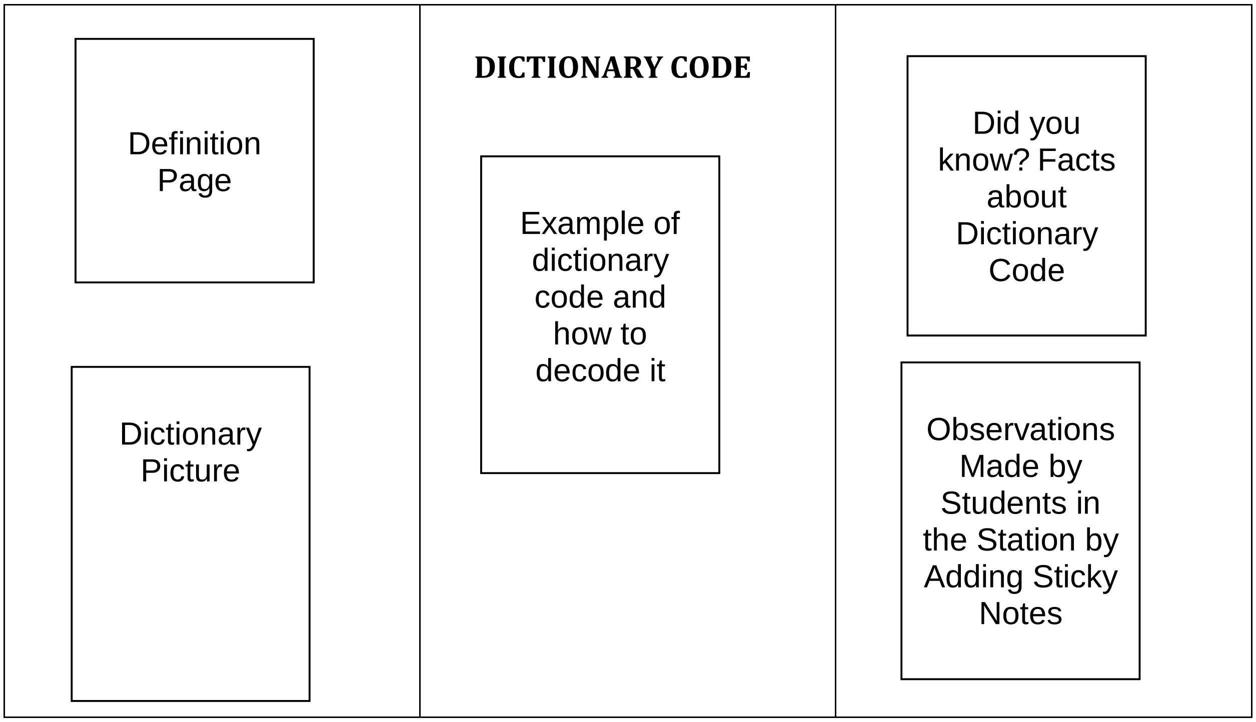
- Worksheet to complete at the Dictionary Code Station

- Student directions for the station

- Frayer vocabulary worksheet for the station

- 2 student dictionaries

Layout of the Dictionary Code Station Board



Definition Page

Dictionary Picture

DICTIONARY CODE

Example of dictionary code and how to decode it

Did you know? Facts about Dictionary Code

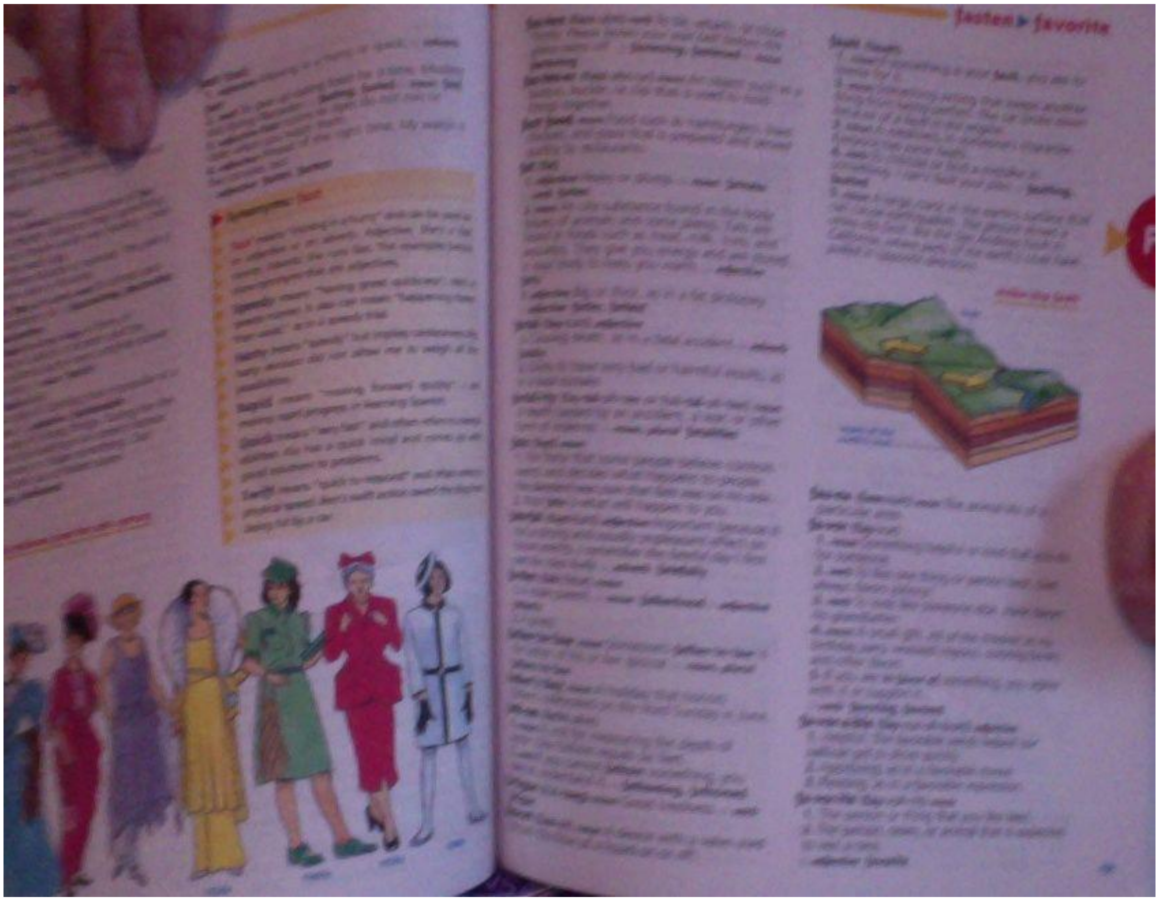
Observations Made by Students in the Station by Adding Sticky Notes

Definition of Dictionary Code

A popular form of book code, it uses numerical code based on page number (which must be 3 digits or 4 depending on how many pages are in the dictionary), column number (one digit) and ordinal location of number in a column for decoding words in a message.(two digits) All dictionary codes then are 6 or 7 digits.

*If the page number is less than 3 digits, then a zero is added at the beginning, and if the position of the word is less than 2 digits, a zero is added at the beginning also.

Example Using a Dictionary Code



fasten ▸ favorite

191106 –

Page number + column number + word numerical position in column = "fatality"

Directions for Dictionary Code

1. Watch the Dictionary Code Slideshare located on the Slideshare app on your iPad.

2. Use the two dictionaries provided at your station and the display board example to complete as many of the self-checking cards for practice. When you and your partner think that you understand how to use the Dictionary Code, you can move on to the next step. You and your partner can work together to solve the riddles on the front of the cards and then check your solution with the correct answer located on the back of the card. If you do not get the right answer, see if you can figure out your mistake. If you need to, ask for help! Mrs. Heiniger is nearby to help!

3. Use the dictionaries to complete the Dictionary Code Sheet in the station. The Dictionary Code sheet will offer you a clue to the identity of an object hidden in the room. Once you have decoded the clue, write the plaintext for your guess about where the object is hidden. Then you will use dictionaries to encode your guess.

4. With your partner, complete the Frayer Method vocabulary sheet to explain your vocabulary word for this station.

5. In your crypto-journal, write at least 2 positive aspects of the shift cipher and at least 2 negative aspects of the Dictionary Code.

6. Put your Dictionary Code form and Frayer Method vocabulary sheet in the completed papers folder and move to the next station on your station card.

Did You Know?

- The dictionary has been the most popular book agents have used to create a Code Book.

- Dictionary code was used in a scandal surrounding the presidential election of 1876.

- There are also "non" secret codes such as zip codes and telephone numbers.

What are your thoughts about the Dictionary Code?

Is it hard? Is it easy? Do you think it is secure? Or any other thoughts you have…

Use the post it notes to write any thoughts you have and post them below! We will use these as part of our discussion later.

Self-Checking Cards for practicing Dictionary Code

This page contains the front of the cards and the next page will be printed on the back.

Directions

Use the dictionaries at your station to decode answers to the following riddles. Write the answers in your crypto-journal and then check them by turning the question card over to find the correct answer!

What gets wetter and wetter the more it dries?

001101 571105

How can a pants pocket be empty and still have something in it?

279109 079203 242207 001101 251110 264209 279109

A man leaves home, turns left three times, only to return home facing two men wearing masks. Who are those two men?

001101 086102 019107 018202 586102

Self-Checking Cards for practicing Dictionary Code

This page contains the back of the cards and the previous page will be printed on the front.

A towel

It can have a hole in it

A catcher and an umpire

Frayer Method Vocabulary Sheet

Definition	Characteristics
Examples	Non-examples

Dictionary Code

Aliquam congue fermen-tum nisl. Mauris accumsan nulla vel diam. Praesent vestibulum molestie lacus. Aenean nonummy hen-drerit mauris. Phasellus porta. Lorem ipsum dolor mauris elit gomao. Lorem ipsum.

DICTIONARY CODE

Below is an encoded clue to the identity of an object hidden in the room. Decode the clue in the space provided by using the dictionaries provided at your station. Write the plaintext of the clue in the space provided.

Encoded Clue:

35928 18623 55216

Write the decoded clue below:

What do you think the object is? (Write your plaintext answer below.)

Now encode your guess to the identity of the object by using the Dictionary Code:

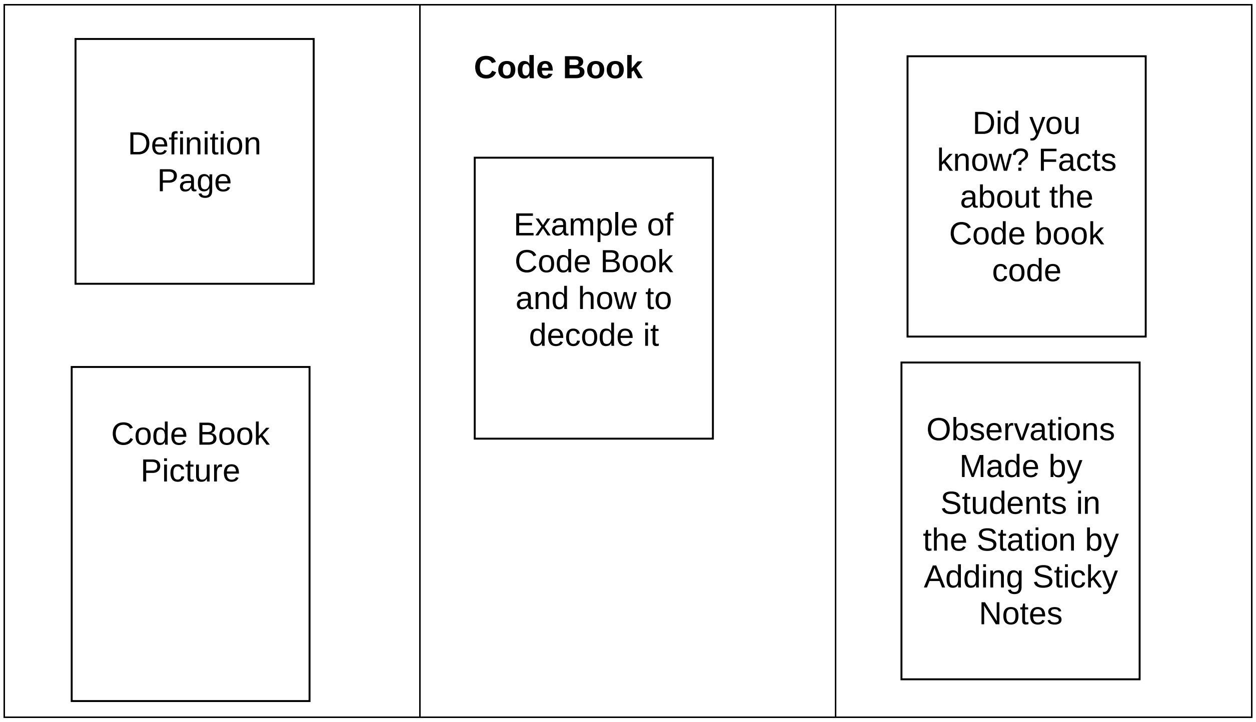
Code Book Code Station

Pages for Display on the Code Book Board

1. Definition
2. Example of Code Book and how to decode it
3. Picture of a Code Book
4. Did you know? Facts about Code Books
5. Student observation page

- Code Book form
- Self-checking cards for practice with the Code Book
- Paper and worksheet to complete at the Code Book station
- Student directions for the station
- Frayer vocabulary worksheet for the station
- Code book
- Clip art image pages (2 sets) –one set already used in Code Book and a second page of "extra" images to be used for new words

Layout of the Code Book Station Board



Definition Page

Code Book Picture

Code Book

Example of Code Book and how to decode it

Did you know? Facts about the Code book code

Observations Made by Students in the Station by Adding Sticky Notes

Definition of Code Books

A codebook is a type of document used for gathering and storing codes. Originally codebooks were often literally books, but today codebook is a word that means the complete record of a series of codes, regardless of what type of format it is in.

Directions for using the Code Book

1. Watch the Code Book Prezi located on the Prezi app on the iPad provided at your station.

2. Use the Code Book provided at your station to complete as many of the self-checking cards for practice. You will need to write down the letters in the code on the paper provided at your station. When you and your partner think that you understand how to use the code book, you can move on to the next step.

3. You and your partner can work together to solve the riddles on the front of the cards and then check your solution with the correct answer located on the back of the card. If you do not get the right answer, see if you can figure out your mistake. If you need to, ask for help! Mrs. Heiniger is nearby to help! To complete this assignment, you will use the Code Book provided at your station.

3. Use the Code Book to complete the Code Book Sheet in the station. The Code Book sheet will offer you a clue to the identity of an object hidden in the room. Once you have decoded the clue, write the plaintext for your guess about where the object is hidden. Then you will use the Code Book to encode your guess. Icon sheets have been provided at your station for you to use to cut and paste your encoded guess on the Code Book sheet. "Extra" icons have been printed for you to use to encode your guess if the words you need to use are not already in the Code Book.

   *Note – there are 2 copies of each icon. You will paste 1 icon into the codebook and write beside it the word that goes with it. You will use the other icon on the Code Book sheet.

5. With your partner, complete the Frayer Method vocabulary sheet to explain your vocabulary word for this station.

6. In your crypto-journal, write at least 2 positive aspects of the shift cipher and at least 2 negative aspects of the Code Book.

7. Put your Code book form and Frayer Method vocabulary sheet in the completed papers folder and move to the next station on your station card.

Did You Know?

- Code books have been around for hundreds of years

- There are two part Code books – 1 book is the *encoding book* and the other book is the *decoding book*

- In 1791 Robert R. Livingston made a 1700 numerical code book listing all of the words he might use to communicate with Thomas Jefferson. Jefferson ran into a problem though while on vacation, when he got a coded message from Livingston because Jefferson had left his code book at home and could not decode the message!

What are your thoughts about Code Books?

Is it hard? Is it easy? Do you think it is secure? Or any other thoughts you have…

Use the post it notes to write any thoughts you have and post them below! We will use these as part of our discussion later.

Frayer Method Vocabulary Sheet

Definition

Characteristics

Code Book

Examples

Non-examples

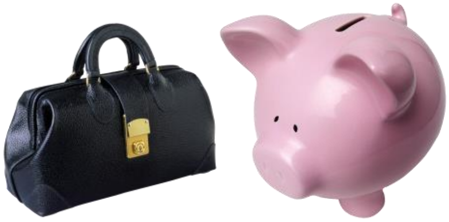
Self-Checking Cards for practicing with The Code Book

This page contains the front of the cards and the next page will be printed on the back.

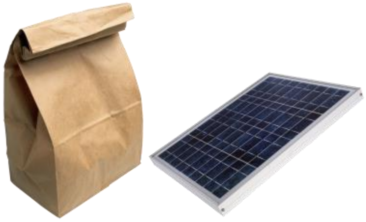
Directions

Use the Code Book at your station to decode answers to the following riddles. Write the answers in your crypto-journal and then check them by turning the question card over to find the correct answer!

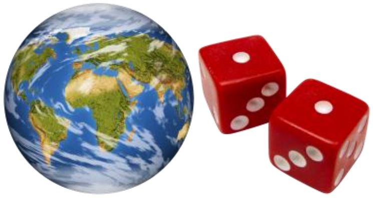
What goes up when rain comes down?



What word contains all of the twenty six letters?



What kind of coat can only be put on when wet?



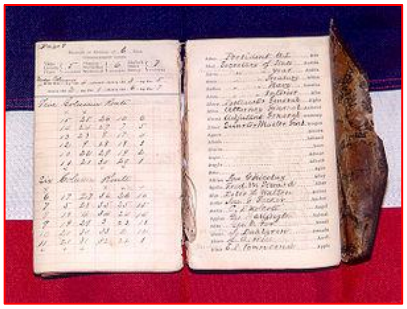
Self-Checking Cards for practicing with The Code Book

This page contains the back of the cards and the previous page will be printed on the front.

An umbrella

The alphabet

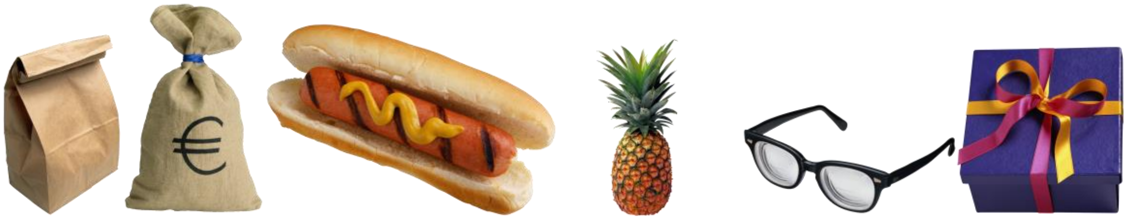
A raincoat



The Code Book

Below is an enciphered clue to the identity of a hidden object in the room. Decode the clue in the space provided by using the Code Book at your station. Write the plaintext of the clue in the space provided.

Encoded clue:

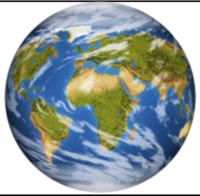
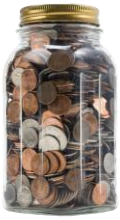
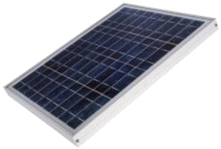
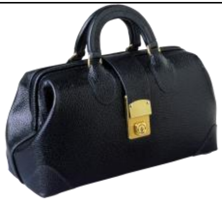
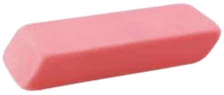
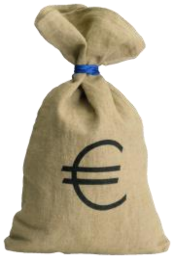
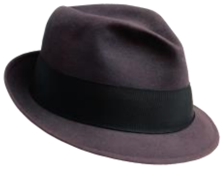
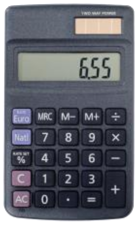


Write the decoded clue below.

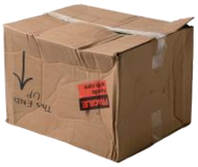
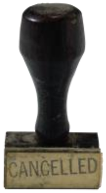
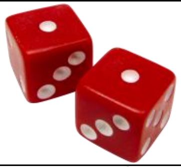
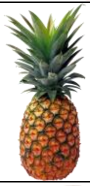
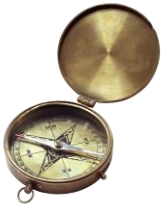
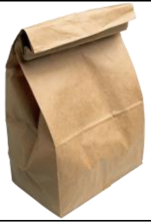
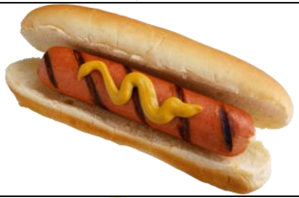
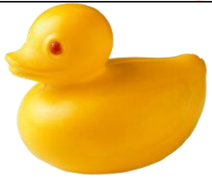
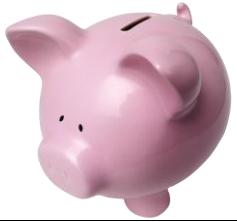
What do you think the object is? (Write your plaintext answer below.)

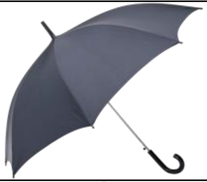
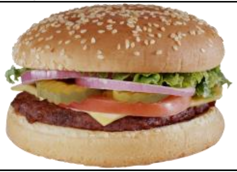
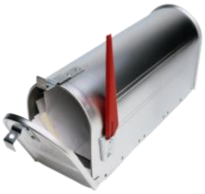
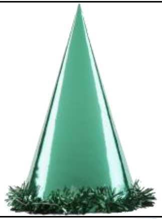
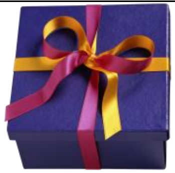
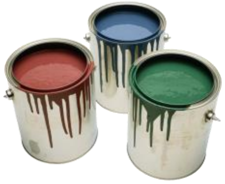
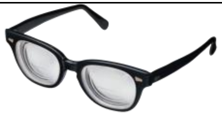
Now encode your guess as to the identity of the object using the Code Book provided. You will cut out the correct icons and paste them on the back of this sheet. The "extra icons" sheet can be used for words that are not in the Code Book or you can draw your own. You will need to cut out 2 of these – paste one here and one in the Code Book. Make sure you write the word it goes with in the Code Book.

Code Book code

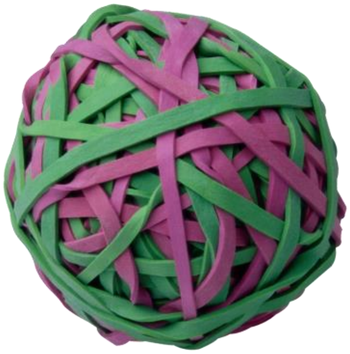
Word	Symbol
A	
All	
Alphabet	
An	
Be	
Better	
Can	
Coat	

Comes	
Contains	
Down	
goes	
Kind	
Letters	
Of	
On	
Only	

Put	
Rain	
Raincoat	
See	
Six	
The	
To	
Twenty	
Umbrella	

Up	
Wet	
What	
When	
With	
Word	
You	

"Extra" icons for you to use for words that do not appear in the Code Book – feel free to draw your own if you wish!

Shift Cipher Station

The following pages contain the pages/handouts/display sheets needed for the Shift Cipher Station. Below is a listing of what is included for this station. The pages that follow have this information in the following order.

- Pages for Display on the Shift Cipher Station Board

  1. Vocabulary
  2. Example of ciphertext using Shift cipher and how to decipher
  3. Picture of a cipher wheel
  4. Did you know? Facts about Shift Ciphers
  5. Student observation pages

- Cipher Wheel form

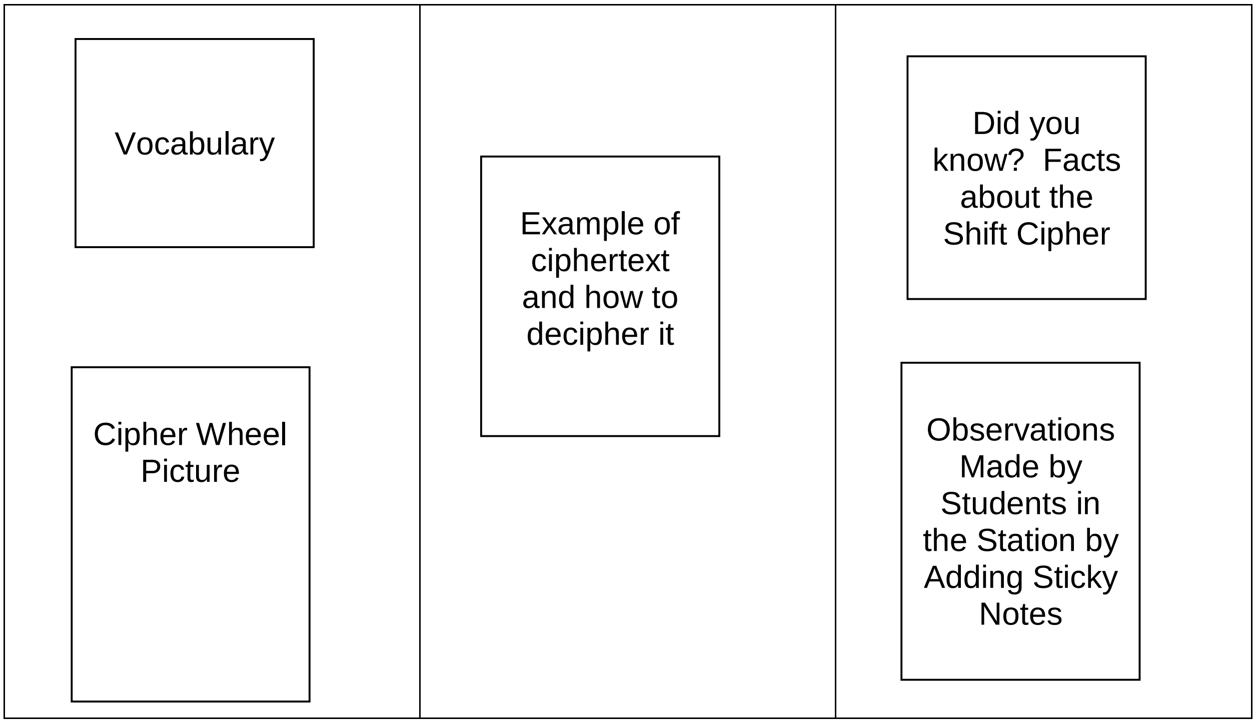
- Self-checking cards for practice with the Shift cipher

- Worksheet to complete at the Shift Cipher Station

- Student directions for the station

- Frayer Method Vocabulary Sheet

Layout of the Shift Cipher Station Board



Vocabulary

Cipher Wheel Picture

Example of ciphertext and how to decipher it

Did you know? Facts about the Shift Cipher

Observations Made by Students in the Station by Adding Sticky Notes

Vocabulary

Plaintext: text as it is normally written

Ciphertext: text that has been enciphered to prevent others from reading it

Cipher: A type of secret writing which replaces each letter in the plaintext with a different letter, number, or symbol

Substitution cipher: A cipher in which the letters of the plaintext stay in the same order, but they are replaced by different letters, numbers, or symbols

Monoalphabetic cipher: a cipher that uses the same ciphertext symbol to represent each plaintext letter throughout the ciphertext

Shift cipher: a type of monoalphabetic cipher which shifts the alphabet by a given number of spaces

Algorithm: Mathematical formula or well-defined steps used to encipher text

Key: A number that is used in the algorithm. In the case of the shift cipher it is the number of spaces the alphabet is shifted.

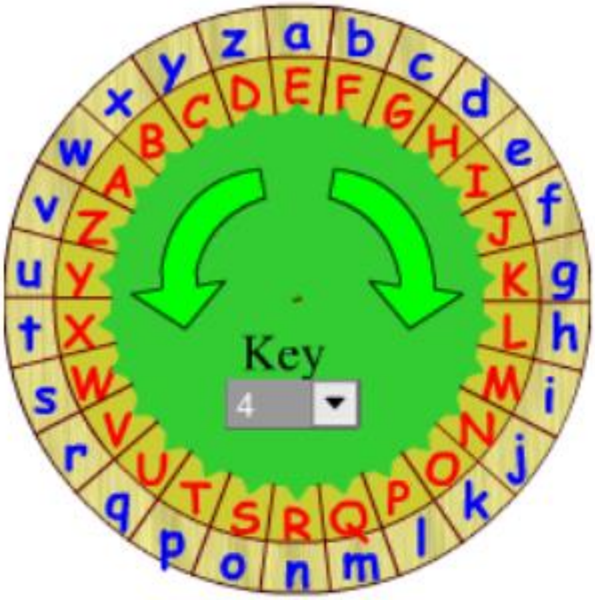
Example Using a Shift Cipher
(Shift of 4)

The shift of 4 means that each letter moves 4 places to the left in the ciphertext alphabet or the cipher wheel moves 4 spaces around.

The plaintext letters are on the top line, and the ciphertext letters are on the bottom line.

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
E	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

The plaintext letters are on the outer circle, and the ciphertext letters are on the inner circle.



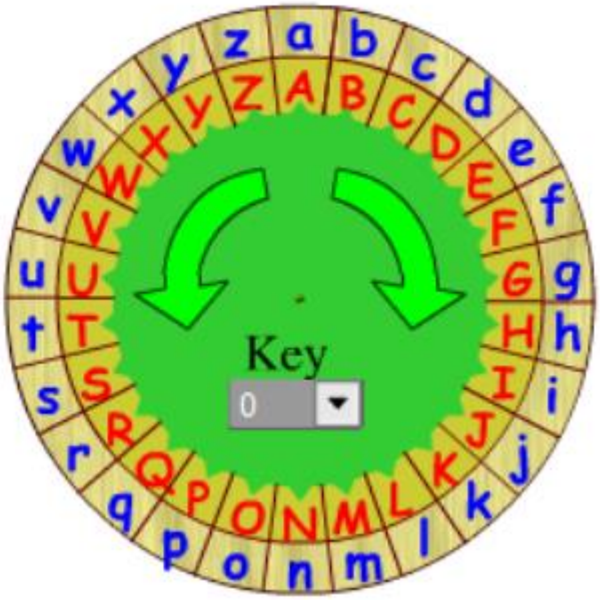
“The way to use the shift cipher” would be enciphered like this
Plaintext: The way to use the shift cipher

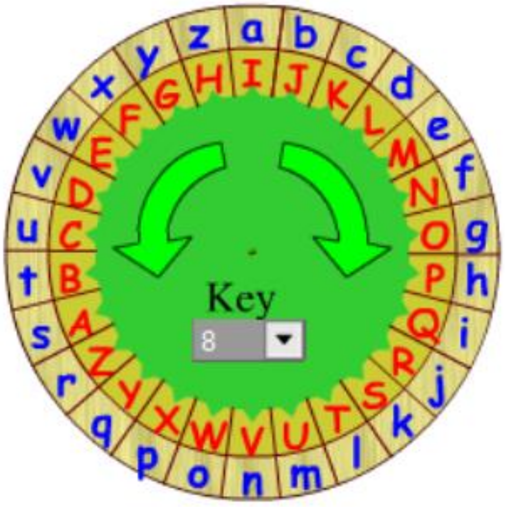
Plaintext	T	H	E		W	A	Y		T	O		U	S	E		T	H	E	
Ciphertext	X	L	I		A	E	C		X	S		Y	W	I		X	L	I	

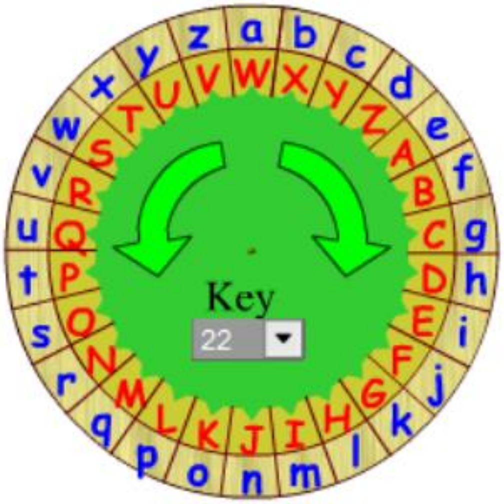
Plaintext	S	H	I	F	T		C	I	P	H	E	R	.
Ciphertext	W	L	M	J	X		G	M	T	L	I	V	

Ciphertext: xli aec xs ywi xli wlmjx gmtliv

Cipher Wheels


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
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
Key
0


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
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 H
Key
8


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
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
Key
22

Did You Know?

- Julius Caesar used a cipher with a key of 3 to shift the letters of the alphabet 3 spaces to the left

- In the Shift Cipher, each plaintext letter is enciphered the same way throughout the text

- A tool called the cipher wheel was invented by Leon Battista Albert around 1466. This tool can be used to encipher a message using the shift cipher.

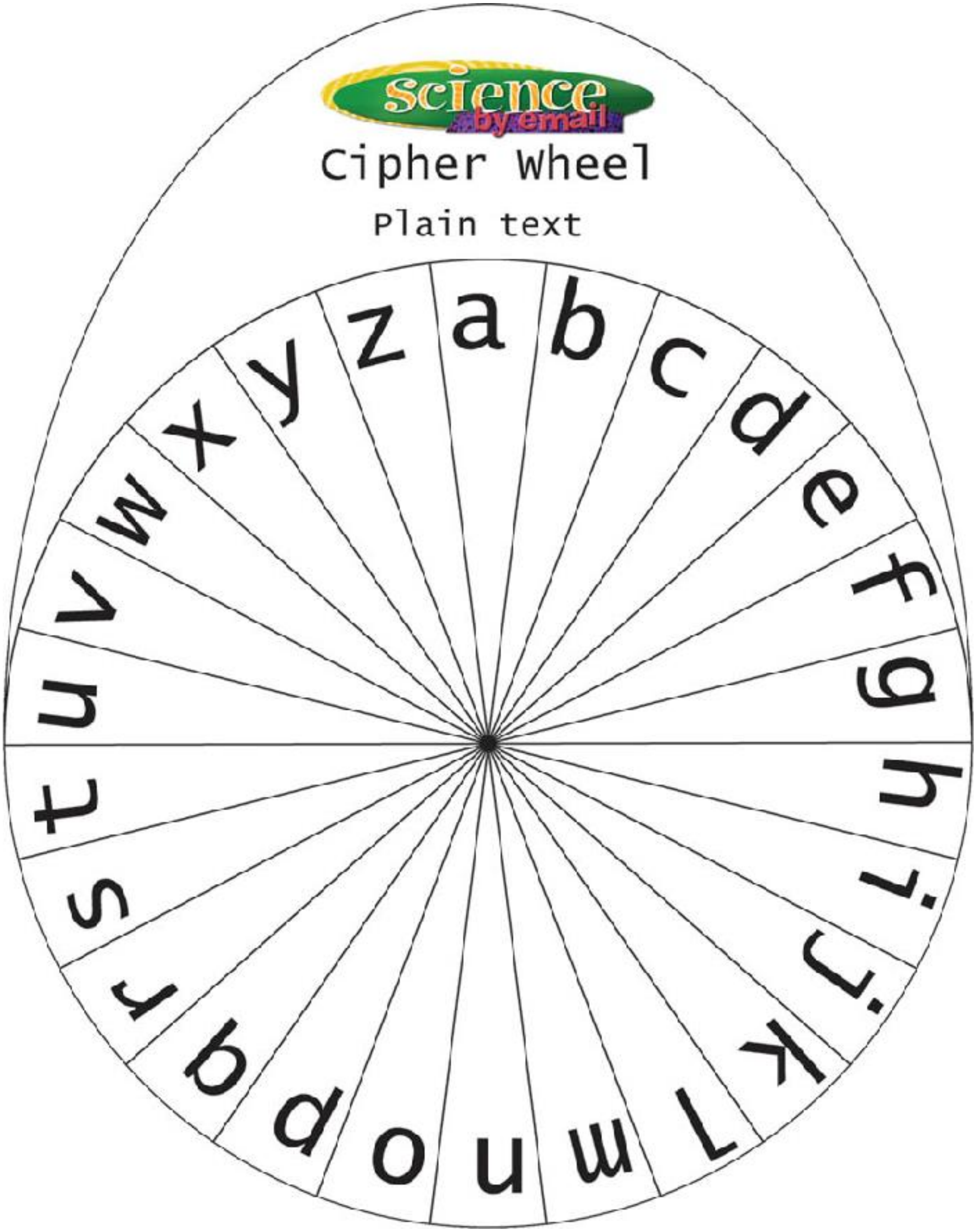
- The cipher key for a shift cipher is easy to remember.

- Shift ciphers are no longer secure when used alone.

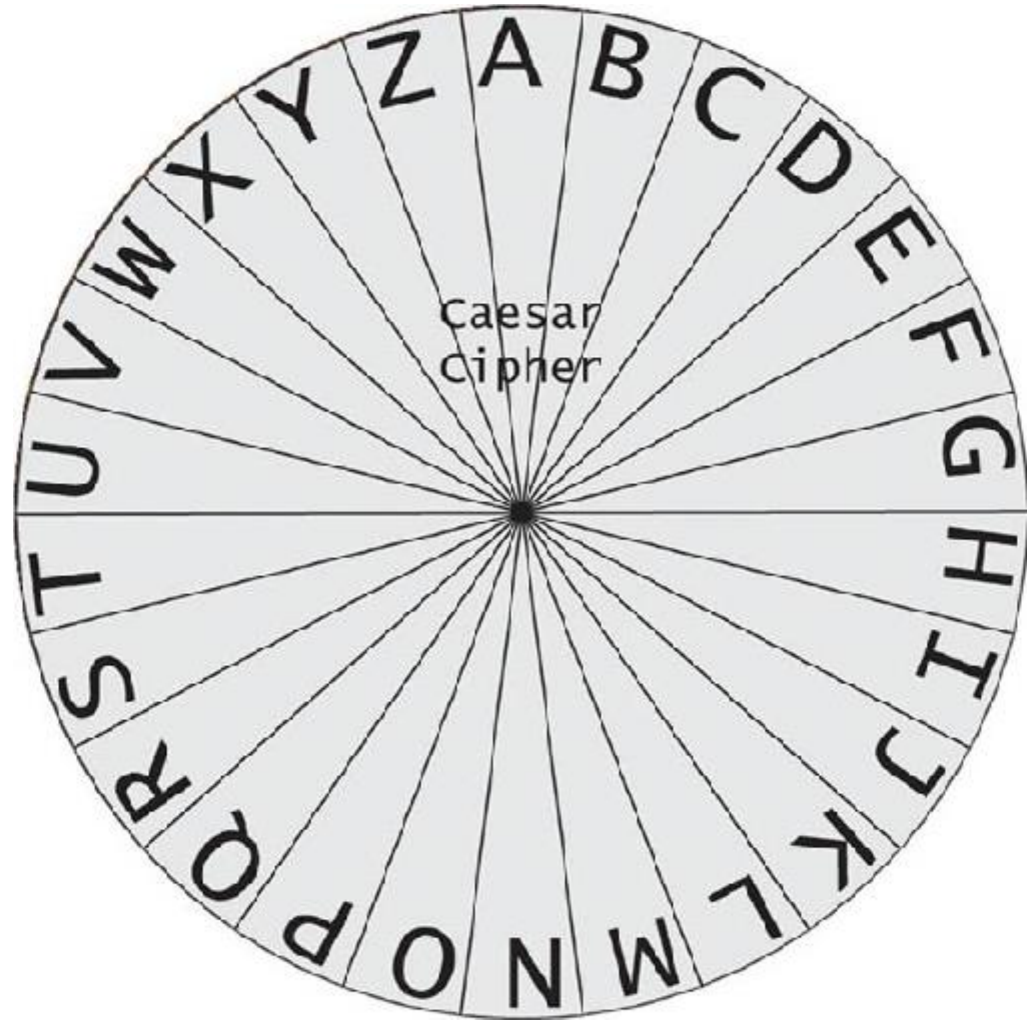
What are your thoughts about the Shift Cipher?

Is it hard? Is it easy? Do you think it is secure? Or any other thoughts you have…

Use the post it notes to write any thoughts you have and post them below! We will use these as part of our discussion later.



Outer Cipher Wheel



Inner Cipher Wheel

Self-Checking Cards for practicing Shift Cipher

This page contains the front of the cards and the next page will be printed on the back.

Directions

Use your cipher wheel or the virtual cipher wheel that has a link on our session website to decipher the ciphertext answers to the following riddles about secrets. Write the answers in your crypto-journal and then check them by turning the question card over to find the correct answer!

Why can't a bank keep a secret?
(Shift of 12)

NQOMGEQ FTQDQ MDQ FAA YMZK FQXXQDE

Why shouldn't you tell a secret on a farm?
(Shift of 20)

VYWUOMY NBY WILH BUM YULM UHX NBY JINUNIYM BUPY YSYM

Why is it difficult to keep a secret when it's cold?
(Shift of 5)

GJHFZXJ DTZW YJJYM HMFYYJW

Self-Checking Cards for practicing Shift Cipher

This page contains the back of the cards and the previous page will be printed on the front.

Because there are too many tellers

Because the corn has ears and the potatoes have eyes

Because your teeth chatter

Shhhh…It's A Secret: Learning the Key to Cryptography
Crypto-Practice for the Shift Cipher

Below is an enciphered clue to the location of a hidden object in the room. Decipher the clue in the space provided by using your cipher wheel or the one you can find at the link on our session website. Write the plaintext of the clue in the space provided.

Enciphered Clue (using a shift of 8):
BW NQVL BPM PQLLMV WJRMKB,

KPMKS NWZ I AMB WN EPMMTA.

BPM MFKQBMUMVB WN NQVLQVO BPM XZQHM QVAQLM

OQDMA UM AWUM PIXXG KPQTTA

Write the deciphered clue below.

Where do you think the object is hidden? (Write your plaintext answer below.)

Now encipher your guess to the location of the object using the shift cipher.
Shift key = ________

Directions
Shift Cipher Station

1. Use the links on our session webpage to visit the two Shift Cipher videos (The web addresses are https://docs.google.com/file/d/0B12_mZTJNpttNC1OSHFGWFlsT1E/edit?pli=1 and http://www.youtube.com/watch?v=GpQeOT0Mqys&feature=youtu.be but you should be able to see them by clicking on "Shift Cipher Video 1" and "Shift Cipher Video 2" on the session website.) View the entire first video and (if you want more information) view the second video from the beginning until the time shows 4:40. (You may watch the rest of the video at home if you want to and have your parents' permission.)
2. Complete as many of the self-checking cards as you need to for practice. When you and your partner think that you understand how to use the shift cipher, you can move on to step 3. You and your partner can work together to solve the riddles on the front of the cards and then check your solution with the correct answer located on the back of the card. If you do not get the right answer, see if you can figure out your mistake. If you need to, ask for help! Mrs. Tuttle is nearby to help! To complete this assignment, you may use one of the cipher wheels in the station or you can use the online cipher wheel. You can find the online, interactive cipher wheel by using the link on our session website ("Interactive Cipher Wheel) or go to the following website cryptoclub.math.uic.edu/shiftcipher/shiftcipher.htm .

3. Use one of the tools mentioned in step #2 to complete the Crypto-Practice Sheet in the station. The crypto-practice sheet will offer you a clue to the location of an object hidden in the room. Once you have deciphered the clue, write the plaintext for your guess about where the object is hidden. Then you will use your tools from step 2 to encipher your guess.

4. With your partner, complete the Frayer Method vocabulary sheet to explain your definition of shift cipher to your partner.

5. In your crypto-journal, write at least 2 positive aspects of the shift cipher and at least 2 negative aspects of the shift cipher.

6. Put your Crypto-practice form and Frayer Method vocabulary sheet in the completed papers folder and move to the next station on your station card.

Frayer Method Vocabulary Sheet

Definition

Characteristics

Shift Cipher

Examples

Non-examples

Pigpen Cipher Station

The following pages contain the pages/handouts/display sheets needed for the Pigpen Cipher Station. Below is a listing of what is included for this station. The pages that follow have this information in the following order.

- Pages for Display on the Pigpen Cipher Station Board

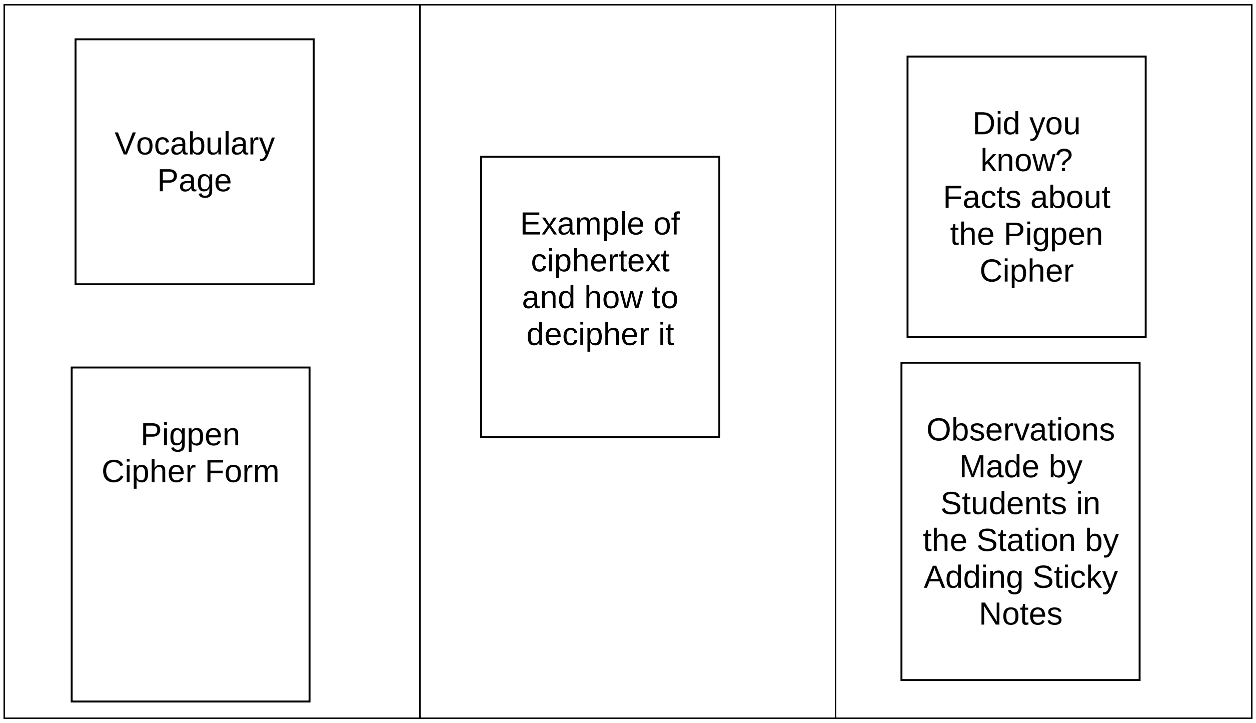
1. Vocabulary
2. Example of ciphertext using the pigpen cipher and how to decipher
3. Picture of Pigpen cipher
4. Did you know? Facts about Pigpen Ciphers
5. Student observation page

- Worksheet to complete at the Pigpen Cipher Station

- Self-checking cards for practice with the Pigpen cipher

- Frayer Method Vocabulary Sheet

Layout of the Pigpen Cipher Station Board


Vocabulary Page
Pigpen Cipher Form
Example of ciphertext and how to decipher it
Did you know? Facts about the Pigpen Cipher
Observations Made by Students in the Station by Adding Sticky Notes

Vocabulary

Plaintext: Text as it is normally written

Ciphertext: Text that has been enciphered to prevent others from reading it

Cipher: A type of secret writing which replaces each letter in the plaintext with a different letter, number, or symbol

Substitution cipher: A cipher in which the letters of the plaintext stay in the same order, but they are replaced by different letters, numbers, or symbols

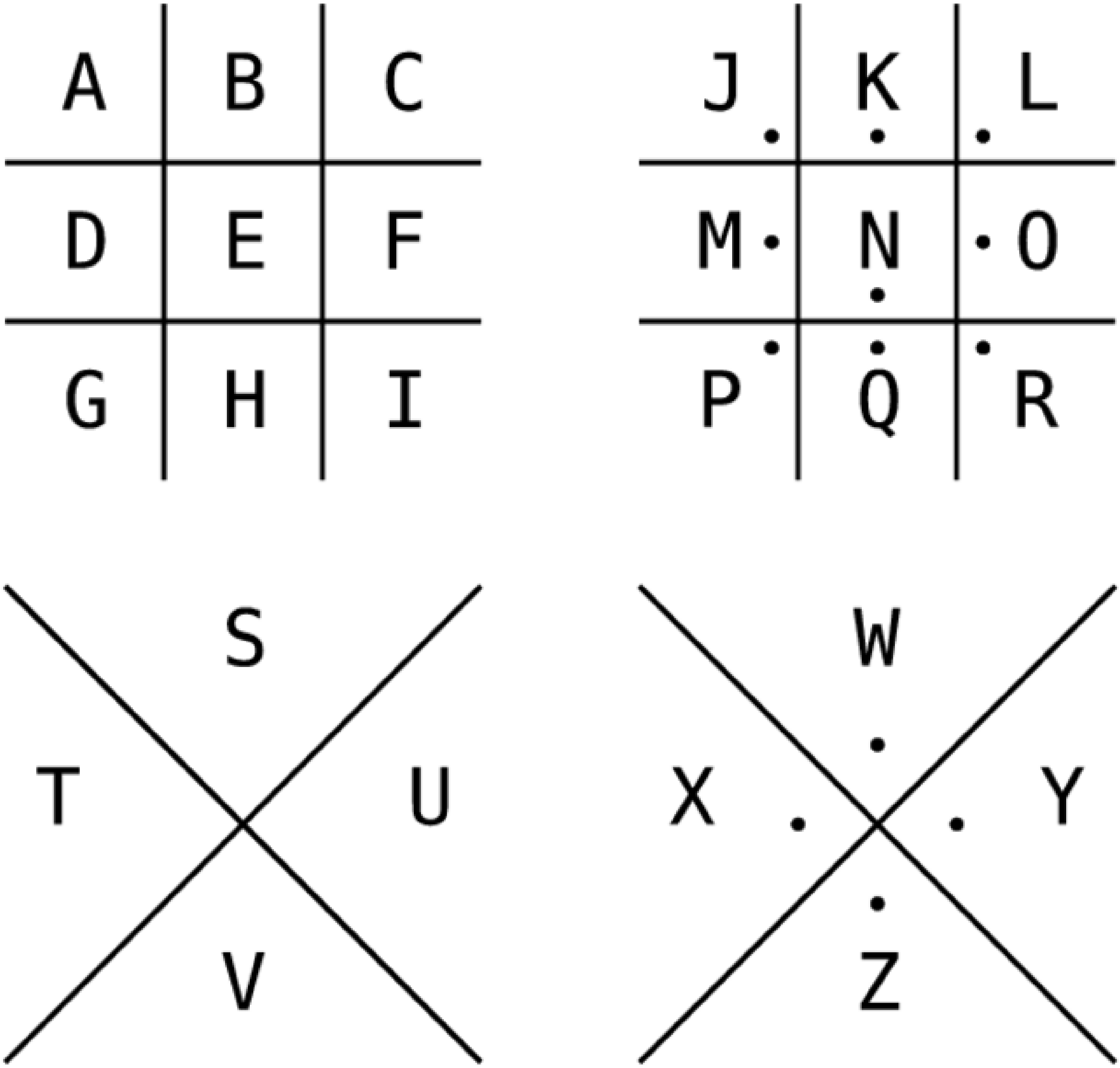
Monoalphabetic cipher: a cipher that uses the same ciphertext symbol to represent each plaintext letter throughout the ciphertext

Pigpen cipher: a type of monoalphabetic cipher which uses a symbol found on the pigpen cipher form to replace each letter of the plaintext

Algorithm: Mathematical formula or well-defined steps used to encipher text

Key: A vital piece of information needed for the algorithm. In the case of the pigpen cipher, the key is the form used to encipher the letters.

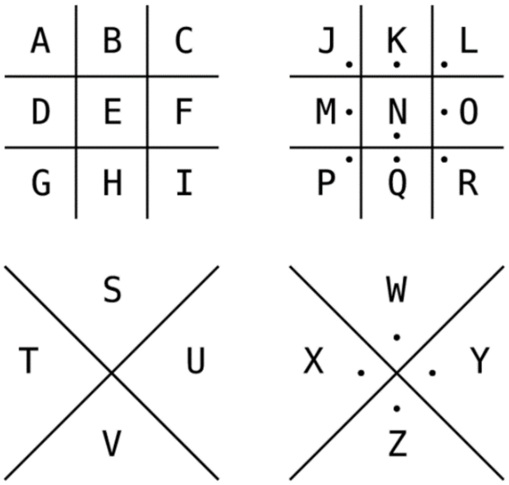
Pigpen Cipher Form



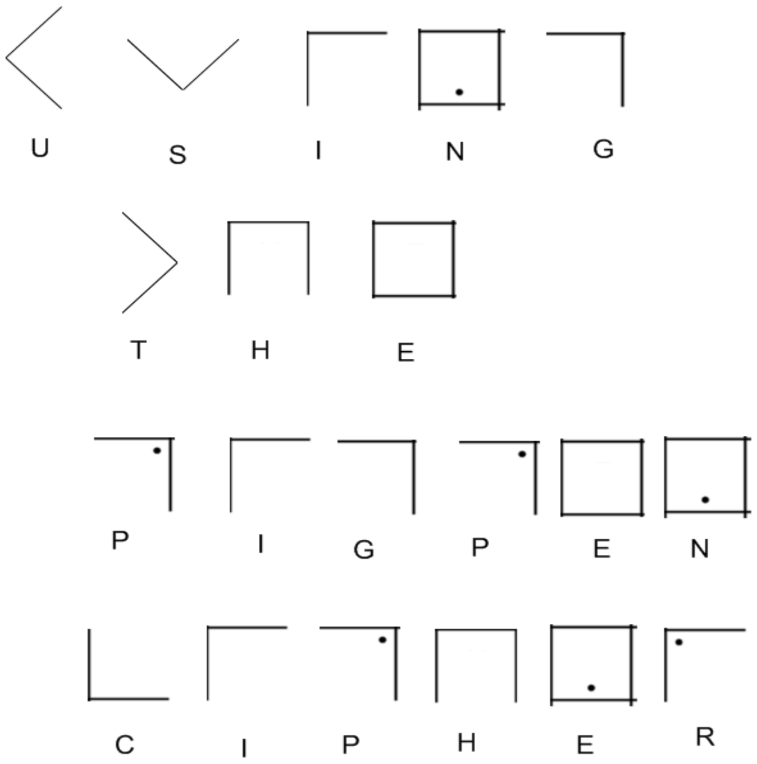
Example Using the Pigpen Cipher

Each letter of the text is enciphered using the symbol that is around that letter in the Pigpen Cipher form

.



“Using the Pigpen Cipher” would look like this



Did you know?

- The Pigpen Cipher got its name because some people thought the form looked like pigpens and the dots looked like little pigs.

- The Pigpen Cipher is also referred to as the Free Mason Cipher because the Free Masons used it.

- The key (the pigpen cipher form) is easy to remember.

- The pigpen cipher form is a tool that can be used to help encipher text using the Pigpen Cipher.

- The pigpen cipher is not secure when used alone.

What are your thoughts about the Pigpen Cipher?

Is it hard? Is it easy? Do you think it is secure? Or any other thoughts you have…

Use the post it notes to write any thoughts you have and post them below! We will use these as part of our discussion later.

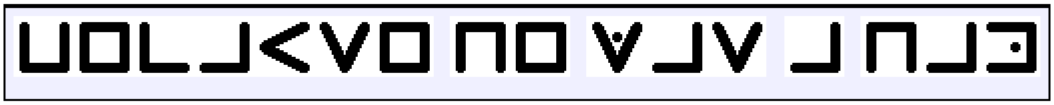
Self-Checking Cards for practicing Pigpen Cipher

This page contains the front of the cards and the next page will be printed on the back.

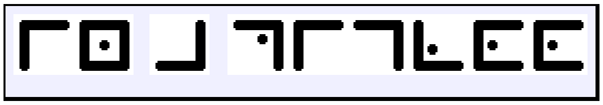
Directions

Use your pigpen cipher form to decipher the ciphertext answers to the following riddles about pigs. Write the answers in your crypto-journal and then check them by turning the question card over to find the correct answer!

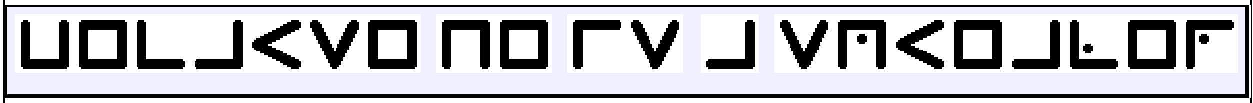
Why did the pig become an actor?



Where does an Eskimo Pig live?



Why shouldn't you tell a secret to a pig?



Self-Checking Cards for practicing Pigpen Cipher

This page contains the back of the cards and the previous page will be printed on the front.

Because he was a ham

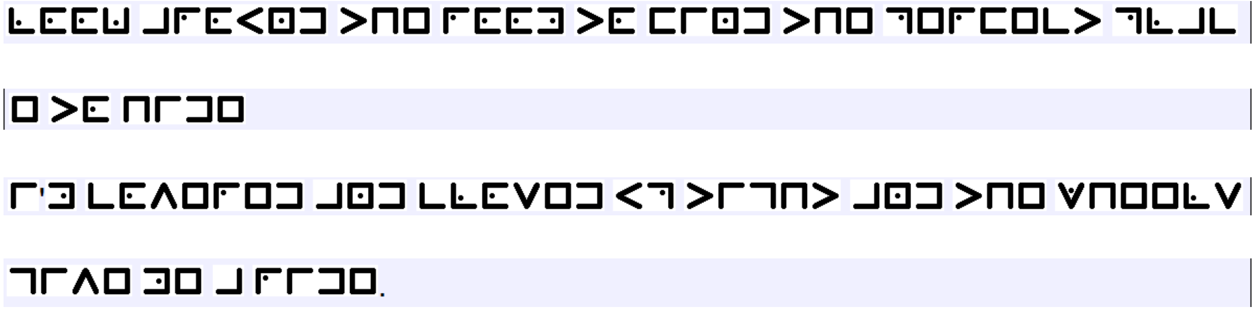
In a pigloo

Because he is a squealer

Shhhh…It's A Secret: Learning the Key to Cryptography
Crypto-Practice for the Pigpen Cipher

Below is an enciphered clue to the location of a hidden object in the room. Decipher the clue in the space provided by using your pigpen cipher form. Write the plaintext of the clue in the space provided.

Enciphered Clue:



Write the deciphered clue below.

Where do you think the object is hidden? (Write your plaintext answer below.)

Now encipher your guess to the location of the object using the pigpen cipher.

Directions
Pigpen Cipher Station

1. Use the link on our session webpage to visit the Pigpen Cipher Prezi. (The web address is http://prezi.com/a-nyaz1-lem9/pigpen-cipher/ but you should be able to see it by clicking on "Pigpen Cipher Prezi" on the session website.) Then watch the Pigpen Cipher video. (The web address is https://drive.google.com/file/d/0B8_Iy2-ce3qlNjdfQnBFZDlhTUU/edit?usp=sharing but you should be able to see it by clicking on "Pigpen Cipher Video" on the session website.)

2. Complete as many of the self-checking cards for practice as you need to in order to make sure that you understand how to use the Pigpen cipher. When you and your partner believe that you understand how to use the cipher, you can move on to step 3. You and your partner can work together to solve the riddles on the front of the cards and then check your solution with the correct answer located on the back of the card. If you do not get the right answer, see if you can figure out your mistake. If you need to, ask for help! Mrs. Tuttle is nearby to help! To complete this assignment, you may use the Pigpen Cipher form in this station. This form shows the symbols that represent each letter of the alphabet.

3. Use the Pigpen cipher form to complete the Crypto-Practice Sheet in the station. The crypto-practice sheet will offer you a clue to the location of an object hidden in the room. Once you have deciphered the clue, write the plaintext for your guess about where the object is hidden. Then you will use your pigpen cipher form to encipher your guess.

4. Complete the Frayer Model Vocabulary sheet for the vocabulary word from this station.

5. Write at least 2 positive aspects and 2 negative aspects of the Pigpen Cipher in your Crypto-journal for this station.

6. Put your Crypto-practice form and your Frayer Model Vocabulary Sheet in the completed papers folder and move to the next station on your station card.

Frayer Method Vocabulary Sheet

Definition	Characteristics
Examples	Non-examples

Pigpen Cipher

Aliquam congue fermentum nisl. Mauris accumsan nulla vel diam. Praesent vestibulum molestie lacus. Aenean nonummy hendrerit mauris. Phasellus porta. Lorem ipsum dolor mauris elit gomao. Lorem ipsum.

DICTIONARY CODE

Answer Key

Below is an encoded clue to the identity of an object hidden in the room. Decode the clue in the space provided by using the dictionaries provided at your station. Write the plaintext of the clue in the space provided.

Encoded Clue:

35928 18623 55216

One eyed telescope

Write the decoded clue below:

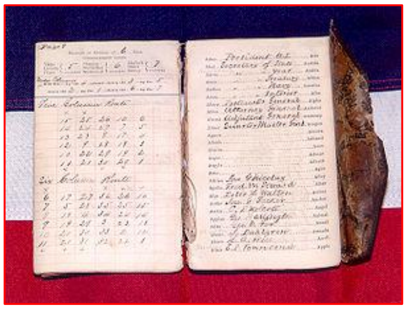
One eyed telescope

What do you think the object is? (Write your plaintext answer below.)

Answers will vary.

Now encode your guess to the identity of the object by using the Dictionary Code:

Answers will vary, but the plaintext above should be encoded correctly. (The correct guess is a spyglass.)

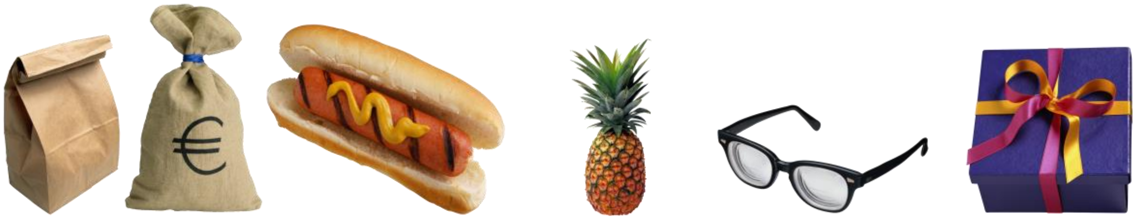


The Code Book

Answer Key

Below is an enciphered clue to the identity of a hidden object in the room. Decode the clue in the space provided by using the Code Book at your station. Write the plaintext of the clue in the space provided.

Encoded clue:



Write the decoded clue below.

The better to see you with

What do you think the object is? (Write your plaintext answer below.)

Answers will vary.

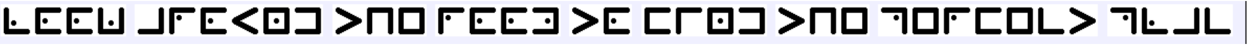
Now encode your guess as to the identity of the object using the Code Book provided. You will cut out the correct icons and paste them on the back of this sheet. The "extra icons" sheet can be used for words that are not in the Code Book or you can draw your own. You will need to cut out 2 of these – paste one here and one in the Code Book. Make sure you write the word it goes with in the Code Book.
Answers will vary, but the plaintext above should be correctly encoded using the code book code provided. (The correct answer is a spyglass.)

Shhhh…It's A Secret: Learning the Key to Cryptography
Crypto-Practice for the Pigpen Cipher

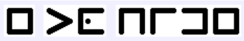
Answer Key

Below is an enciphered clue to the location of a hidden object in the room. Decipher the clue in the space provided by using your pigpen cipher form. Write the plaintext of the clue in the space provided.

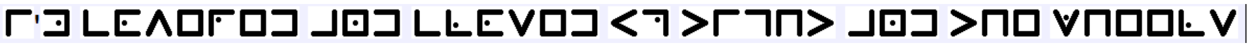
Enciphered Clue:



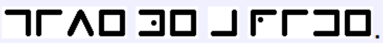
Look around the roomto find the perfect plac



eto hide



Im covered andc losed uptight and the wheels



give mea ride

Write the deciphered clue below.
Look around the room to find the perfect place to hide.
I'm covered and closed up tight, and the wheels give me a ride.

Where do you think the object is hidden? (Write your plaintext answer below.)

Answers will vary,

Now encipher your guess to the location of the object using the pigpen cipher.

Answers will vary but the plaintext above should be enciphered correctly.

The object is located in a blue bag with wheels.

Shhhh…It's A Secret: Learning the Key to Cryptography
Crypto-Practice for the Shift Cipher
Answer Key

Below is an enciphered clue to the location of a hidden object in the room. Decipher the clue in the space provided by using your cipher wheel or the one you can find at the link on our session website. Write the plaintext of the clue in the space provided.

Enciphered Clue (using a shift of 8):
BW NQVL BPM PQLLMV WJRMKB,
TO FIND THE HIDDEN OBJECT,
KPMKS NWZ I AMB WN EPMMTA.
CHECK FOR A SET OF WHEELS.
BPM MFKQBMUMVB WN NQVLQVO BPM XZQHM QVAQLM
THE EXCI TEMENT OF FIND ING THE PR I Z E INSIDE
OQDMA UM AWUM PIXXG KPQTTA
GI V E S ME SO ME HAPPY CHI L LS

Write the deciphered clue below.
To find the hidden object, check for a set of wheels.
The excitement of finding the prize inside gives me some happy chills!

Where do you think the object is hidden? (Write your plaintext answer below.)

Answers will vary.

Now encipher your guess to the location of the object using the shift cipher.
Shift key = ________

Answers will vary but the enciphered text should match the plaintext above.

The object is located in a blue bag with wheels.

Assessment Rubrics (Day 1)

Station Assessments

	Did not attempt activity (0 pts.)	Partially completed the activity (1 pt.)	Completely finished the activity but contained more than 5 errors (2 pts.)	Completely finished the activity but the response contained 1-5 errors (3 pts.)	Completely finished the activity with no errors (4 pts.)
First Station Decipher Clue Activity					
First Station Encipher Guess Activity					
Second Station Decipher Clue Activity					
Second Station Encipher Guess Activity					
Total					/16

Positive and Negative Aspects Assessment

	Student did not attempt (0 pts.)	Student listed only one positive or one negative aspect (1 pt.)	Student listed only one positive and one negative aspect (2 pts.)	Student only listed 3 aspects instead of 4 (3 pts.)	Student listed 2 positive aspects and 2 negative aspects (4 pts.)
First Cryptosystem					
Second Cryptosystem					
Total					/8

LESSON #2
More Tools in Your Cryptographic Toolkit

I. DEFINE OBJECTIVES AND CONTENT	
LESSON OBJECTIVE	The learner will use at least two different established cipher systems to encipher and decipher information and will explain at least two positive aspects and two negative aspects of each of those systems.
POINT TO PONDER	When creating a cryptosystem, the time needed to decipher a message should be considered as important as the algorithm used to make the system secure.
ESSENTIAL QUESTION	How have codes and ciphers of the past helped us create more perfect cryptosystems today?

CONTENT Outline the content you will teach in this lesson.	A. Spoken codes 1. Navajo code--Code Talkers a) Used during WWII by the allies b) Code was never broken 2. Pig Latin 3. Turkish Irish 7. Ciphers A. Control interactions among people since only those who know the key can understand and participate in the communication B. A type of secret writing which replaces each letter in the text with a different letter, number, or symbol C. Vocabulary 1. Algorithm a) Mathematical formula for converting text b) Well defined steps followed to encipher text 2. Key a) Number that is used in the algorithm b) Word that is used as a guide to encipher and decipher text D. Transposition Ciphers 1. The letters in the plaintext are not changed 2. The letters of the plaintext are rearranged to hide the meaning of the enciphered text 3. Examples a) Rail fence cipher (1) Named because the placement of the letters during the transposition resemble a rail fence (2) Used during the Civil War b) Route cipher (1) Letters of the text are written in a grid and rearranged following a predetermined route (2) No evidence exists that this type of cipher was broken during the Civil War although it was used often 4. Advantages a) Requires a long time for someone to break the cipher by hand because there are a lot of different combinations of letter positions possible b) The ciphertext which results from the transposition cipher makes no sense. 5. Disadvantages a) Susceptible to deciphering by computer

b) Not highly secure because the letters do not change

E. Polyalphabetic ciphers

1. Uses different ciphertext characters to represent the same plaintext character in the same enciphered message
2. Examples

a) Alberti Cipher

(1) Created in 1466 in Florence, Italy by Leon Battista Alberti

(2) Uses a cipher wheel

(a) Two concentric circles with a common center and the smaller one on top of the larger one

(b) Twenty-six sections go around the circumference of each circle--one for each letter of the alphabet

(c) The letters of the alphabet are written in order around the edge of the surface of each circle

(d) The circles are rotated to line the plaintext letters (on the outer circle) with their ciphertext letters (on the inner circle)

(3) The letter that aligns with the letter a on the cipher wheel is indicated in the cipher by a capital letter

(4) After a few words are enciphered, the wheel is rotated to pair the plaintext letters and ciphertext letters differently

b) Vigenére Cipher

(1) Created in 1586 by Blaise de Vigenére who combined the works of Leon Battista Alberti and Johannes Trithemius

(2) Uses a tableau (like Trithemius's) which is a list of 26 alphabets down the page with each successive alphabet's letters shifted one place to the left

(3) Uses a key word to indicate the order in which the alphabets will be used to encipher text

3. Advantages

a) More difficult to break than monoalphabetic ciphers because if a single ciphertext letter is known it cannot be substituted throughout the ciphertext because it may represent different letters at different times

b) Not susceptible to frequency analysis

4. Disadvantages

a) If the key is short and the text is long, the length of the key may be determined and the cipher broken

b) Using the key again makes it less secure

8. Jobs involving cryptography

A. Cryptanalysts

1. Analyze the security of cryptographic projects

2. Break cryptosystems

B. Cryptosystem designers

1. Create complex algorithms called cryptographic systems to use to encipher information

2. Work for technology companies and governments

C. Cryptographic engineers

1. Use cryptography to solve human problems

2. Typically address issues of data confidentiality, data integrity, and the authentication of people and devices

D. Digital rights professionals

1. Ensure the security of copyrighted digital materials

2. Use cryptographic keys to "scramble" information so that it cannot be illegally copied

E. University professors

1. Perform research in cryptography

2. Teach others about cryptography

II. PRE-PLANNING	
What will students UNDERSTAND as a result of this lesson? How does this connect to the Essential Question?	Students will understand that each cryptosystem has weaknesses and strengths. Through this understanding, students will realize that working to resolve and overcome the weaknesses of cryptosystems from the past and building on their strengths has allowed cryptographers to create better, more secure code and cipher systems.

What will students be able to DO as a result of this lesson?	Students will be able to encipher plaintext and decipher ciphertext using at least two additional cryptosystems. Students will be able to list at least two positive aspects and two negative aspects of each of the cryptosystems they study today.

III. PLANNING	
HOOK Describe how you will grab students' attention at the beginning of the lesson. BE CREATIVE.	TIME: 3 min Nancy will greet student with spoken code (a form of Pig Latin) as they enter the classroom. The students will try to decode what is being said. During this time, Carol will encourage students to listen carefully to the code and try to determine what Nancy is saying. After students have had 1-2 minutes to try to understand the code, we will ask the students to tell whether they had a hard time or easy time understanding the code. We will briefly relate this to how understanding the code or not understanding the code would have an impact on the **INTERACTIONS** among people (connection to the theme). We will also discuss how students who didn't understand the code felt when they could not participate in this **INTERACTION** by understanding what was being said.
INSTRUCTION Explain Step-by-step what you will do in this lesson. Be explicit about ties to Points to Ponder, Essential Question, and Interactions here. Include ALL support and teaching materials with your unit.	TIME: 64 min. 1. After the hook, we will discuss (as a class) spoken codes and how they have been used. After allowing students the opportunity to share any spoken codes they are familiar with, we will briefly discuss the Navajo Code talkers code used during WWII that was never broken, Pig Latin, and Turkish Irish. We will discuss the fact that these codes are pretty easy to understand when they are written, but when they are spoken quickly, they can confuse others. We will discuss how these spoken codes affect the **INTERACTIONS** between and among people (theme). (3 min) 2. Return crypto-journals to students. 3. What type of jobs use cryptography today? We will place cards around the room that contain job titles that use cryptography today—cryptanalysts, cryptosystem designers, cryptosystem engineers, and digital rights professionals (see attached). With a partner, students will walk around the room and spend 60 seconds at each card writing what they believe the duties would be for each of the job holders. At the end of 4 minutes, when students have visited all the cards, we will discuss their thoughts and what the actual job duties are. We will also mention university professors and the duties of that job. How do each of these jobs affect the **INTERACTIONS** that people have with one another (theme)? (7 min) 4. Students will review their Day 1 vocabulary words on their iPad with the Quizlet app and with the addition of these two new words: polyalphabetic cipher, transposition

cipher. (5 minutes) At each of their stations today, they will complete a Frayer vocabulary sheet for their station: Rail Fence Cipher, Route Transposition Cipher, Alberti Cipher and Vigenére Cipher.

5. Students will attend their first assigned station with their station partner and rotate to a new one as they finish. The stations below will run simultaneously. Each student should complete at least two stations. Cryptosystem creation team members will complete different stations so that they can share information with one another and incorporate all ideas into their final product.
6. As students work in each of the stations, the teachers will be available to discuss their work, answer questions, and guide informal discussions with each group that will help them see possible positive aspects and negative aspects of each system as well as how knowledge of these positive and negative aspects could be used to create a better, more secure cryptosystem (essential question). We will also discuss the time it takes the students to decipher the messages in each of the stations. We will discuss what the students think is more important—considering the time it takes to encipher and decipher messages or making sure that the algorithm is complicated and secure (point to ponder).

Station 1 (approx. 20 min)

Rail Fence Cipher

1. Students will view the video http://www-tc.pbs.org/wgbh/nova/assets/swf/1/cryptography/cryptography.swf to learn how the Rail Fence Transposition Cipher uses a scrambled pattern to encipher and decipher information.
2. Students will use the Rail Fence directions and coded message cards (see attached) provided at this station to practice this method.
3. Using their knowledge of the rail fence cipher, the students will decipher a clue to the identity of a hidden object in the room. They will then use the rail fence cipher to encipher their guess as to the identity of the hidden object. (see attached)
4. Students will complete the Frayer Model sheet to explain their definition and understanding of the Rail Fence Cipher.
5. In their crypto-journal, the students will write at least 2 positive aspects and 2 negative aspects of the Rail Fence Cipher.

6. A miniature display board will be provided at this station to reinforce the information provided to them on the video. (see attached)
   Clue: What signers need
   Object: Pen

Station 2 (approx. 20 min)

Route Cipher

1. Student will view the video http://www-tc.pbs.org/wgbh/nova/assets/swf/1/cryptography/cryptography.swf to learn how the route transposition cipher uses a pre-determined route to encipher and decipher messages.
2. Students will use the route cipher directions and the enciphered message cards (see attached) provided at this station to practice this method.
3. Students will use the route transposition cipher to decipher the clue to the identity of the secret object. They will then use the cipher to encipher their guess as to the identity of the hidden object. (see attached)
4. Students will complete the Frayer Model sheet to explain their definition and understanding of the Route Cipher.
5. In their crypto-journal, students will write at least 2 positive aspects and 2 negative aspects of the Route Cipher.
6. A miniature display board will be provided at this station to reinforce the information provided to them on the video (see attached)
   Clue: A script writer tool
   Object: Pen

Station 3 (approx. 20 min)

Alberti Cipher

1. Student will view the Prezi located at http://prezi.com/u3cfwjb38slk/?utm_campaign=share&utm_medium=copy and the video located at https://drive.google.com/file/d/0B8_Iy2-ce3qlbzJvREF2dGlmdTQ/edit?usp=sharing to learn about the Alberti cipher and how the Alberti cipher uses the cipher disk to encipher and decipher information.
2. Students will use their provided Alberti cipher disk (see attached) to decipher and encipher the texts located on the self-checking cards (see attached). They will solve as many cards as necessary to make sure they understand the cipher.
3. Students will use their Alberti cipher disk to decipher the clue to the location of the secret object for today. They will then use the tool to encipher their guess as to the location of the hidden object (see attached Crypto-practice sheet).

4. Students will complete the Frayer Model sheet to explain their definition and understanding of the Alberti Cipher (see attached).
5. In their crypto-journal, students will write at least 2 positive aspects of the Alberti Cipher and 2 negative aspects of the Alberti Cipher.
6. A display board will be in the station to reinforce the information already presented and provide additional information about the Alberti Cipher.

Station 4 (approx. 20 min)

Vigenére Cipher

1. We will provide each student with a Vigenére tableau that lists the 26 alphabets needed to create a Vigenére Cipher. Students will then view the video located at http://www.youtube.com/watch?v=K1SuiUu4kG0 until the timer reads 3:08. Then they will watch the video located at http://www.youtube.com/watch?v=9ZU5WHvYTGM until they believe that they understand how to encipher text using the Vigenére tableau. (The second video is a very slow moving video. It should not be necessary to watch the entire video for the students to understand how to encipher the message using the Vigenére cipher.)
2. Students will complete as many of the self-checking cards as necessary to feel comfortable with the skill before they move on to the assessment in step 3. To complete the self-checking cards, students will use the Vigenére tableau.
3. Students will use the supplied Vigenére tableau or the interactive one located at http://www.mathman.gr/component/content/article/10/639-cryptography-Vigenére-cipher.html to decipher the clue to the location of the secret object. They will then use their chosen tableau form to encipher their guess as to the location of the hidden object.
4. Students will complete the Frayer Model sheet to explain their definition and understanding of the Vigenére Cipher (see attached).
5. In their crypto-journal, students will write at least 2 positive aspects of the Vigenére Cipher and 2 negative aspects of the Vigenére Cipher.
6. A display board will be in the station to reinforce the information already presented and provide additional information about the Vigenére Cipher.

7. We will reassemble as a group and discuss the students' experiences with the ciphers. As a class, we will discuss what

	the students found to be easy or hard at each station. We will also discuss their thoughts about the ciphers and, since they have now completed these stations and have more experience, the students' thoughts about the point to ponder and the essential question. (4 min.) 8. Students will meet with their cryptosystem partner and discuss the different systems they experienced at the stations. With their partner, students will brainstorm the parts of each of the cryptosystems (from both days) that they might want to incorporate into their cryptosystem. The students will record any important information they might use for their cryptosystem in their crypto-journal and will begin to write their own code or cipher system with their partner in their crypto-journal. (5 min.)
ASSESSMENT (Performance Task) What will the students DO to demonstrate that they have mastered the content? Be specific and include actual assessment with unit materials.	TIME: 3 min. In each station, students will complete a crypto-practice sheet to demonstrate their knowledge of deciphering and enciphering (using the cryptosystem discussed in each station) by deciphering a clue to the location or identity of a hidden object and enciphering their guess about the location or identity of the hidden object. Since they will be visiting at least two stations, this will demonstrate their knowledge of enciphering and deciphering using at least two cipher systems. In each station, students will write at least 2 positive aspects of the cryptosystem and at least 2 negative aspects of the cryptosystem in their crypto-journal. We will collect these journals at the end of each session for assessment purposes. Students will have the opportunity to add the positive aspects and negative aspects they noted about each cryptosystem they experienced to our class padlet.

DOES THE ASSESSMENT ALLOW YOU TO DETERMINE WHETHER OR NOT THE STUDENTS HAVE MET YOUR STATED LESSON OBJECTIVE? [✓ YES] OR NO

ASSESSMENT AND INSTRUCTIONAL MATERIALS
Insert ALL materials here including Assessments and Instructional Materials.
Explicitly LIST any additional files for this lesson. Be sure that ALL materials have been submitted for this lesson.

Files and links needed for this lesson:

(All of these links are located on our session website and, whenever possible, the videos or other instruction are embedded on the website. They are also listed in the lesson plan at the appropriate places.)

Rail Fence Cipher Video
http://www-tc.pbs.org/wgbh/nova/assets/swf/1/cryptography/cryptography.swf

Route Transposition Cipher Video
http://www-tc.pbs.org/wgbh/nova/assets/swf/1/cryptography/cryptography.swf

Alberti Cipher Prezi
http://prezi.com/u3cfwjb38slk/alberti-cipher/?utm_campaign=share&utm_medium=copy

Alberti Cipher Video
https://docs.google.com/file/d/0B8_Iy2-ce3qlbzJvREF2dGlmdTQ/edit?pli=1

Vigenére Cipher Video 1
http://www.youtube.com/watch?v=K1SuiUu4kG0

Vigenére Cipher Video 2
http://www.youtube.com/watch?v=9ZU5WHvYTGM

Interactive Vigenére Tableau
http://www.mathman.gr/component/content/article/10/639-cryptography-vigenere-cipher.html

Padlet for Day 2
http://padlet.com/wall/7ws9ibi3dk

Attachments for Day 2:

Cryptanalysts

Cryptosystem Designers

Cryptosystem Engineers

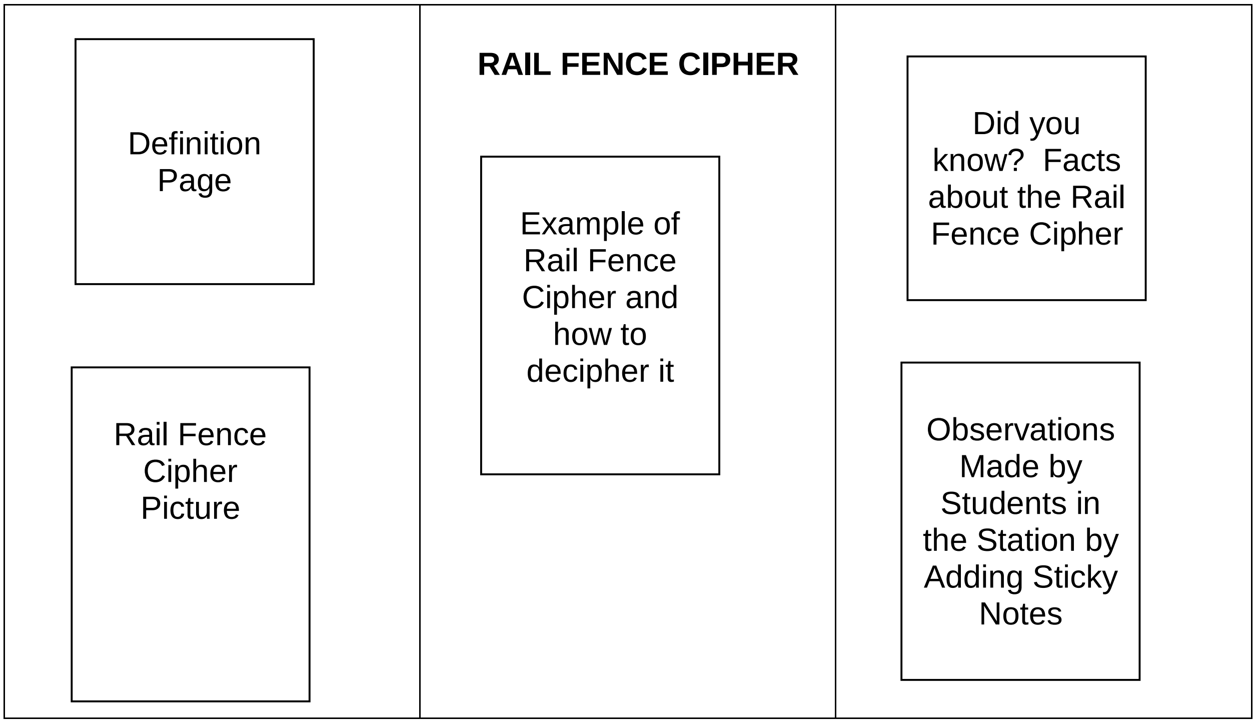
Digital Rights Professionals

- Pages for Display on the Rail Fence Cipher Board

1. Definition
2. Example of Rail Fence Cipher and how to decipher it
3. Picture of a Rail Fence Cipher
4. Did you know? Facts about Rail Fence Cipher
5. Student observation pages

- Rail Fence Cipher form
- Self-checking cards for practice with the Rail Fence Cipher
- Worksheet to complete at the Rail Fence Cipher Station
- Student directions for the station
- Graph paper for creating their Rail Fence Cipher response
- Frayer vocabulary worksheet for the station

Layout of the Rail Fence Cipher Station Board



Definition Page

Rail Fence Cipher Picture

RAIL FENCE CIPHER

Example of Rail Fence Cipher and how to decipher it

Did you know? Facts about the Rail Fence Cipher

Observations Made by Students in the Station by Adding Sticky Notes

Definition of Rail Fence Cipher

A cipher whereby the letters are scrambled in a certain way to make it impossible to read unless you know how they were scrambled.

Example Using a Rail Fence Cipher

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

In a Rail Fence Cipher the message is written in a zigzag pattern with a Code of 3 which means there are 3 rows in the grid. This message enciphered reads:

WECRLTE ERDSOEEFEAOC AIVDEN

When deciphered in a Zigzag pattern the plaintext of the message is as follows:

We are discovered flee at once.

Did You Know?

- The Rail Fence Cipher was first used in the Middle Ages and was used extensively during the Civil War.

- The Rail Fence Cipher gets its name from a bird's eye view of a fence

- The Chevron pattern in clothing and other items that is so popular today, imitates the Rail Fence Cipher pattern.

What are your thoughts about the Rail Fence Cipher?

Is it hard? Is it easy? Do you think it is secure? Or any other thoughts you have…

Use the post it notes to write any thoughts you have and post them below! We will use these as part of our discussion later.

Directions for Rail Fence Cipher

1. Use the link on our session webpage to visit the Rail Fence Cipher video. (The web addresses for the video is http://www-tc.pbs.org/wgbh/nova/assets/swf/1/cryptography/cryptography.swf

2. Use the graph paper provided to complete as many of the self-checking cards as you need to for practice. You and your partner can work together to solve the riddles on the front of the cards and then check your solution with the correct answer located on the back of the card. If you do not get the right answer, see if you can figure out your mistake. If you need to, ask for help! Mrs. Heiniger is nearby to help! To decipher your riddles, use the graph paper provided at your station. When you understand the cipher and believe you can correctly use it, you may move on to the Rail Fence sheet

3. Use the graph paper to complete the Rail Fence Cipher in the station. The Rail Fence Cipher sheet will offer you a clue to the identity of an object hidden in the room. Once you have deciphered the clue, write the plaintext for your guess about where the object is hidden. Then you will use graph paper to encipher your guess.

4. Complete the Frayer Method sheet in the station by explaining the vocabulary word on it with your partner.

5. Write two positive aspects and two negative aspects about the Rail Fence Cipher in your crypto-journal.

6. Put your Crypto-practice form and your Frayer method sheet in the completed papers folder and move to the next station on your station card.

Self-Checking Cards for practicing Rail Fence Cipher

This page contains the front of the cards and the next page will be printed on the back.

Directions

Use the Rail Fence Cipher directions and the graph paper provided at your station to decipher the following riddles. Write the answers in your crypto-journal and then check them by turning the question card over to find the correct answer!

What goes up but never comes down? Key = 3

YAORGUE

How could a cowboy ride into town on Friday, stay two days and ride out on Friday? Key = 3

HOIMRYIHRESAEFIASSNDD

A lawyer, plumber and a hat maker were walking down the street. Who had the biggest hat? Key = 3

TNTEGHXHOEIHHBGETEDEWTISA

Self-Checking Cards for practicing Rail Fence Cipher

This page contains the back of the cards and the previous page will be printed on the front.

Your age

His horse is named Friday

The one with the biggest head

R F E H
A L E C C P E
I N I R

Below is an enciphered clue to the identity of a hidden object in the room. Decipher the clue in the space provided by using the graph paper at your station. Write the plaintext of the clue in the space provided.

Enciphered clue: key = 3

WSEEHTINRNEAGSD

Write the deciphered clue below.

What do you think the object is? (Write your plaintext answer below)

Now encipher your guess as to the identity of the object using the graph paper provided. (Include the key and if you are using nulls in your guess)

Frayer Method Vocabulary Sheet

Definition

Characteristics

Rail Fence Cipher

Examples

Non-examples

- Pages for Display on the Route Transposition Cipher Board

1. Definition
2. Example of Route Transposition Cipher and how to decipher it
3. Picture of a Route Transposition Cipher
4. Did you know? Facts about Route Transposition Cipher
5. Student observation pages

- Route Transposition Cipher form

- Self-checking cards for practice with the Route Transposition Cipher

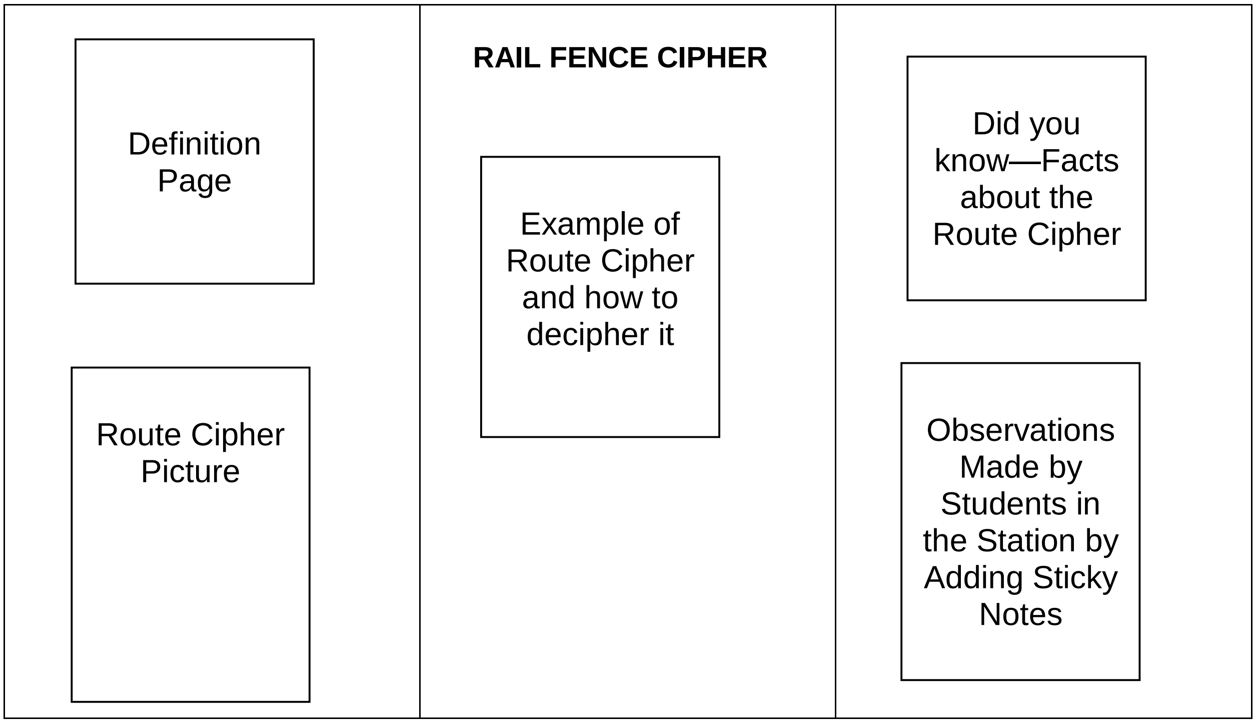
- Worksheet to complete at the Route Transposition Station

- Student directions for the station

- Graph paper for creating their Route Transposition response

- Frayer vocabulary worksheet for the station

Layout of the Route Transposition Cipher Station Board



Definition Page

Route Cipher Picture

RAIL FENCE CIPHER

Example of Route Cipher and how to decipher it

Did you know—Facts about the Route Cipher

Observations Made by Students in the Station by Adding Sticky Notes

Definition of Route Transposition Cipher

A cipher that follows a pre-decided route, either horizontally, vertically or in a spiral

Example Using a Route Transposition Cipher

In a Route Transposition Cipher, the message is enciphered in a route that is determined by the sender. The receiver must know the route pattern in order to decipher it. In this example the route follows a vertical pattern:

The enciphered message reads:
HOOOOWWWWBNXNRCX

To decipher the message, follow the vertical route:

H	O	O	O
O	W	W	W
W	B	N	X
N	R	C	X

How now brown cow

Did You Know?

- Any type of cipher that follows a "route" is called a Route Cipher.

- Route Ciphers include "nulls" which are letters that take up space in the "route" but are not part of the message

What are your thoughts about the Route Transposition Cipher?

Is it hard? Is it easy? Do you think it is secure? Or any other thoughts you have…

Use the post it notes to write any thoughts you have and post them below! We will use these as part of our discussion later.

Self-Checking Cards for practicing Route Transposition Cipher

This page contains the front of the cards and the next page will be printed on the back.

Directions

Use the Route Transpositon Cipher directions and the graph paper provided at your station to decipher the following riddles. Write the answers in your crypto-journal and then check them by turning the question card over to find the correct answer!

I have keys but no locks. I have space but no room. You can enter but you can't go outside. What am I? Key = vertical path, 3 x 3 grid

AYAKBREOD

What two things can you never eat for breakfast? Key = vertical path, 4 x 4 grid

LHDEUAIRNNNXCDNX

How do you share 34 apples among 33 people? Key = spiral path (start writing in the middle) 5 x 5 grid. Go up 1 then to the right. Work clockwise. Read horizontally.

SAPAIWEEEOUMAPUTMEHTHCLKY

Self-Checking Cards for practicing Route Cipher

This page contains the back of the cards and the previous page will be printed on the front.

A keyboard

Lunch and dinner

You make applesauce with them

Route Transposition Cipher

Below is an enciphered clue to the identity of a hidden object in the room. Decipher the clue in the space provided by using the graph paper at your station. Write the plaintext of the clue in the space provided.

Enciphered clue: key = 5 x 5 spiral grid – USES NULLS

OIXXXOIPTXTRAWXSCSRXRETIX

Write the deciphered clue below.

What do you think the object is? (Write your plaintext answer below.)

Now encipher your guess as to the identity of the object using the graph paper provided. (Include the key in your guess)

Directions for Route Cipher

1. Use the link on our session webpage to visit the Route Transposition Cipher video. (The web addresses for the video is http://www-tc.pbs.org/wgbh/nova/assets/swf/1/cryptography/cryptography.swf

2. Use the graph paper provided to complete as many of the self-checking cards as you need to for practice. You and your partner can work together to solve the riddles on the front of the cards and then check your solution with the correct answer located on the back of the card. If you do not get the right answer, see if you can figure out your mistake. If you need to, ask for help! Mrs. Heiniger is nearby to help! To decipher your riddles, use the graph paper provided at your station. When you understand the cipher and believe you can correctly use it, you may move on to the Route Transposition Cipher sheet

3. Use the graph paper to complete the Route Transposition Cipher clue in the station. The Route Transposition Cipher sheet will offer you a clue to the identity of an object hidden in the room. Once you have deciphered the clue, write the plaintext for your guess about where the object is hidden. Then you will use graph paper to encipher your guess.

4. Complete the Frayer Method sheet in the station by explaining the vocabulary word on it with your partner.

5. In your crypto-journal, write at least 2 positive aspects and 2 negative aspects of the Route Cipher.

6. Put your Crypto-practice form and your Frayer method sheet in the completed papers folder and move to the next station on your station card.

Frayer Method Vocabulary Sheet

Definition

Characteristics

Route Transposition Cipher

Examples

Non-examples

Alberti Cipher

The following pages contain the pages/handouts/display sheets needed for the Alberti Cipher Station. Below is a listing of what is included for this station. The pages that follow have this information in the following order.

- Pages for Display on the Alberti Cipher Station Board

1. Vocabulary
2. Example of ciphertext and how to decipher
3. Pictures of cipher disks
4. Did you know? Facts about Alberti Ciphers
5. Student observation pages

- Cipher Wheel form—used to make cipher disks

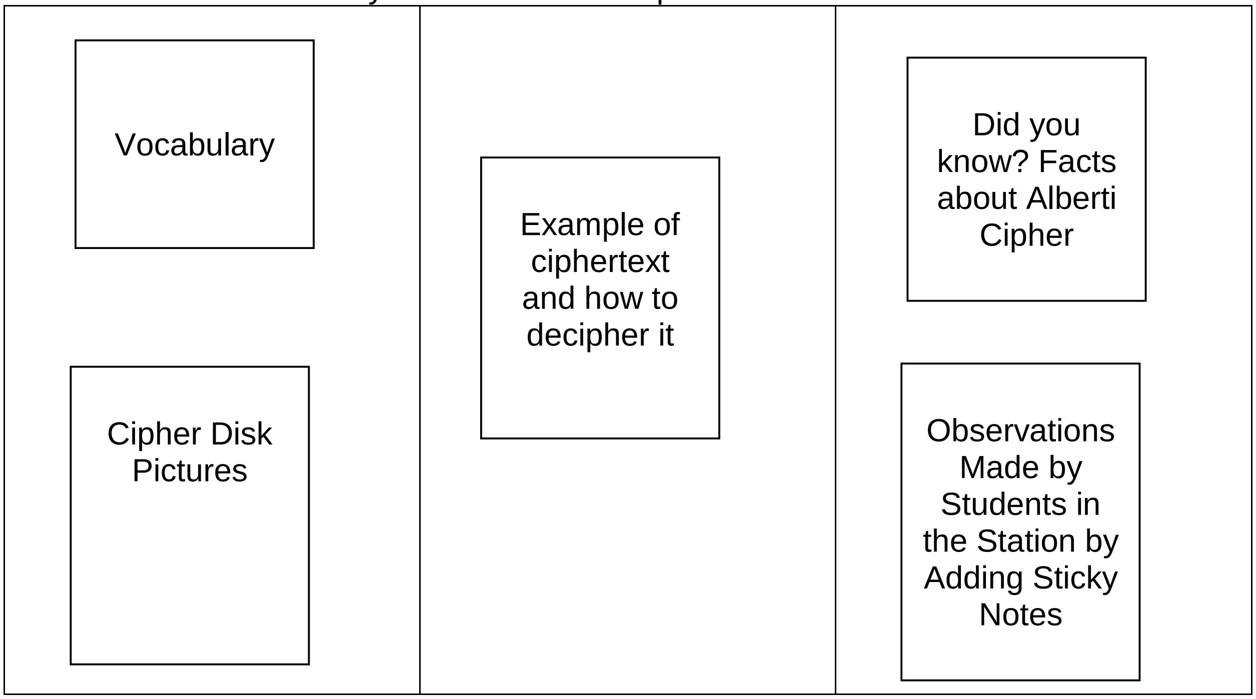
- Self-checking cards for practice with the Alberti cipher

- Worksheet to complete at the Alberti Cipher Station

- Student directions for the station

- Frayer Method Vocabulary Sheet

Layout of the Alberti Cipher Station Board



Vocabulary

Cipher Disk Pictures

Example of ciphertext and how to decipher it

Did you know? Facts about Alberti Cipher

Observations Made by Students in the Station by Adding Sticky Notes

Vocabulary

Plaintext: Text as it is normally written

Ciphertext: Text that has been enciphered to prevent others from reading it

Cipher: A type of secret writing which replaces each letter in the plaintext with a different letter, number, or symbol

Polyalphabetic cipher: a cipher that uses different ciphertext symbols to represent a given plaintext letter within the same ciphertext message

Alberti Cipher: a type of polyalphabetic cipher which uses a cipher disk to pair the letters of the alphabet with other ciphertext letters and then changes the pairing during the enciphering of the text

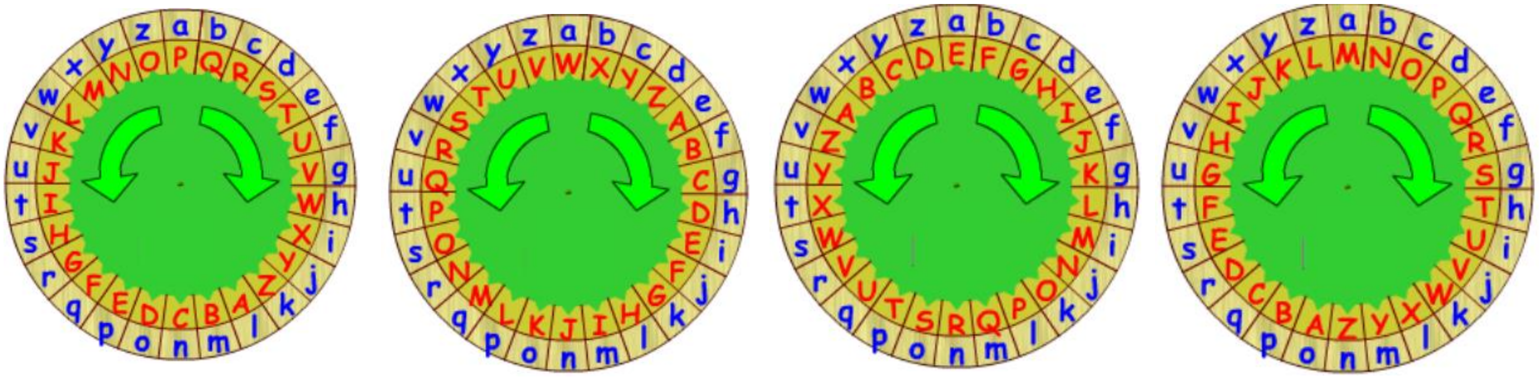
Algorithm: Mathematical formula or well-defined steps used to encipher text

Key: An important piece of information needed for the algorithm. In the Alberti cipher, the key is contained in the ciphertext as capital letters that indicate the way the cipher disk is aligned.

Example Using an Alberti Cipher

Our message is
"Cracking a polyalphabetic cipher is harder than cracking a monoalphabetic cipher."

We will use the cipher disk in the four positions below. Each time we move to a different cipher disk, we will write a capital letter in the ciphertext that will indicate which wheel to use. The capital letter used to indicate which disk to use will be the letter on the inner circle that lines up with the letter "A" on the outer circle.

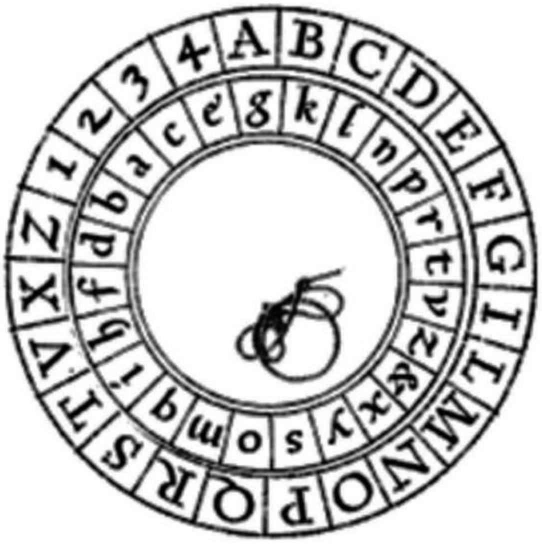

a b c d e f g h i j k l m n o p q r s t u v w x y z
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
a b c d e f g h i j k l m n o p q r s t u v w x y z
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
a b c d e f g h i j k l m n o p q r s t u v w x y z
E F G H I J K L M N O P Q R S T U V W X Y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

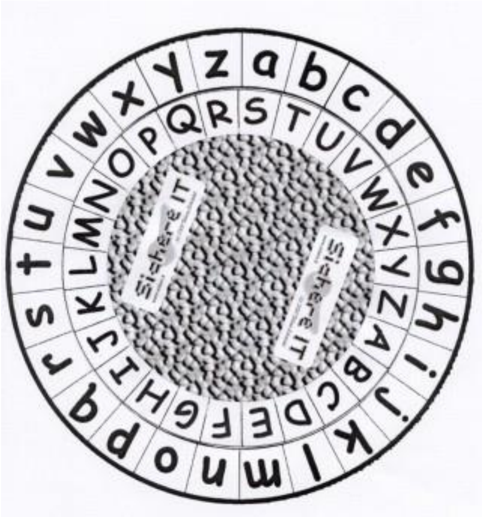
	C	R	A	C	K	I	N	G	A	P	O	L	Y	A	L	P	H	A	B	E	T	I	C		C	I	P	H	E
P	r	g	p	r	z	x	c	v	p	e	d	a	n	p	a	e	w	p	q	t	i	x	r	W	y	e	l	d	a

R	I	S	H	A	R	D	E	R		T	H	A	N	C	R	A	C	K	I	N	G	A		M	O	N	O	A	L
n	e	o	d	w	n	z	a	n	E	x	l	e	r	g	v	e	g	o	m	r	k	e	M	y	a	z	a	m	x

P	H	A	B	E	T	I	C	C	I	P	H	E	R
b	t	m	n	q	f	u	o	o	u	b	t	q	d

Cipher Disks





Did You Know?

- The Alberti Cipher was revolutionary because it changed the pairings of ciphertext and plaintext letters during the same message

- The Alberti Cipher was created by Leon Battista Alberti in 1466 in Florence, Italy

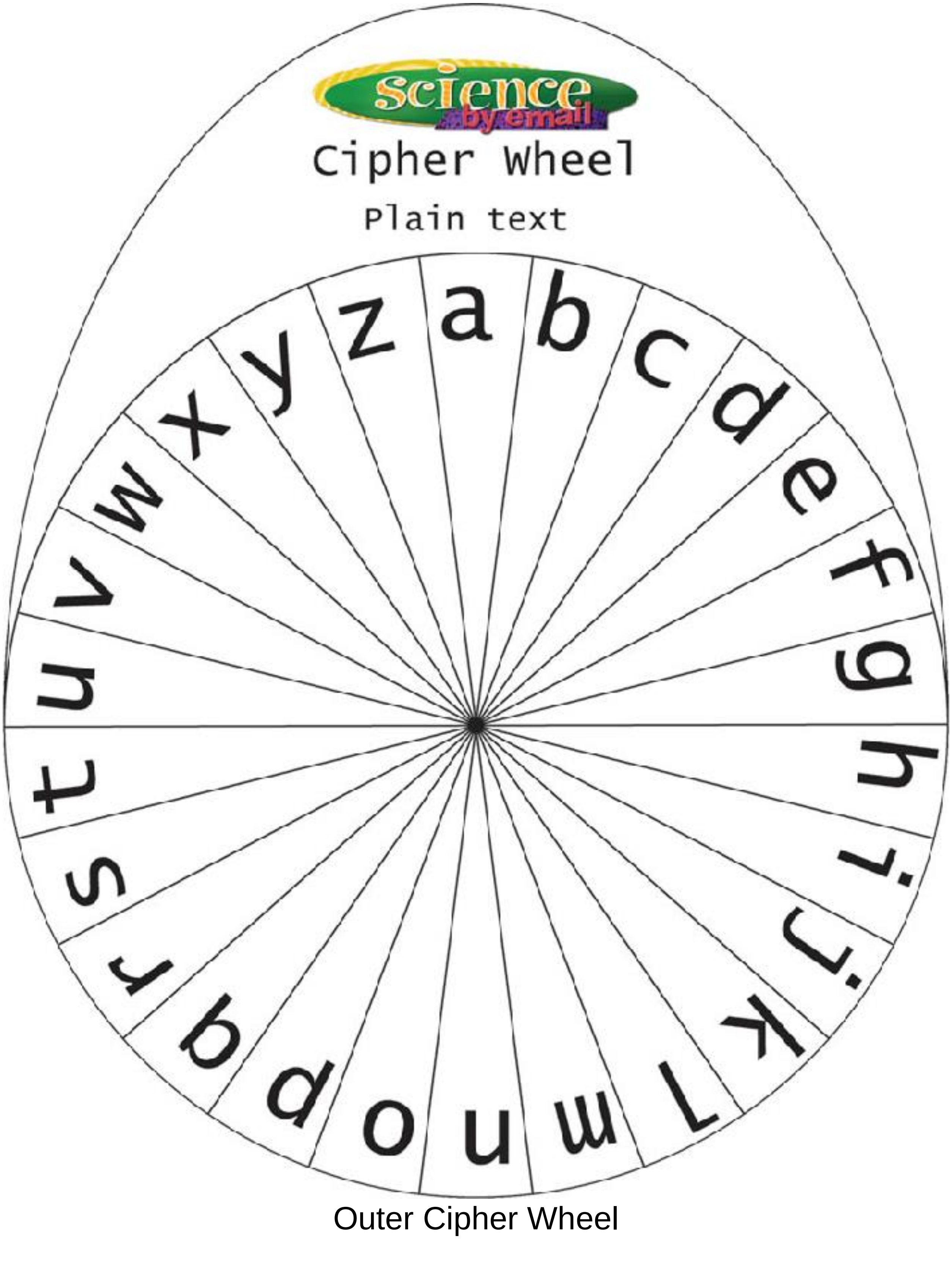
- The Alberti Cipher can be made more secure by changing the order of the alphabet on the inner circle

- The Alberti Cipher can be made more secure if you can find a way not to have to write a capital letter in the ciphertext to indicate how the inner circle position on the cipher disk is changed.

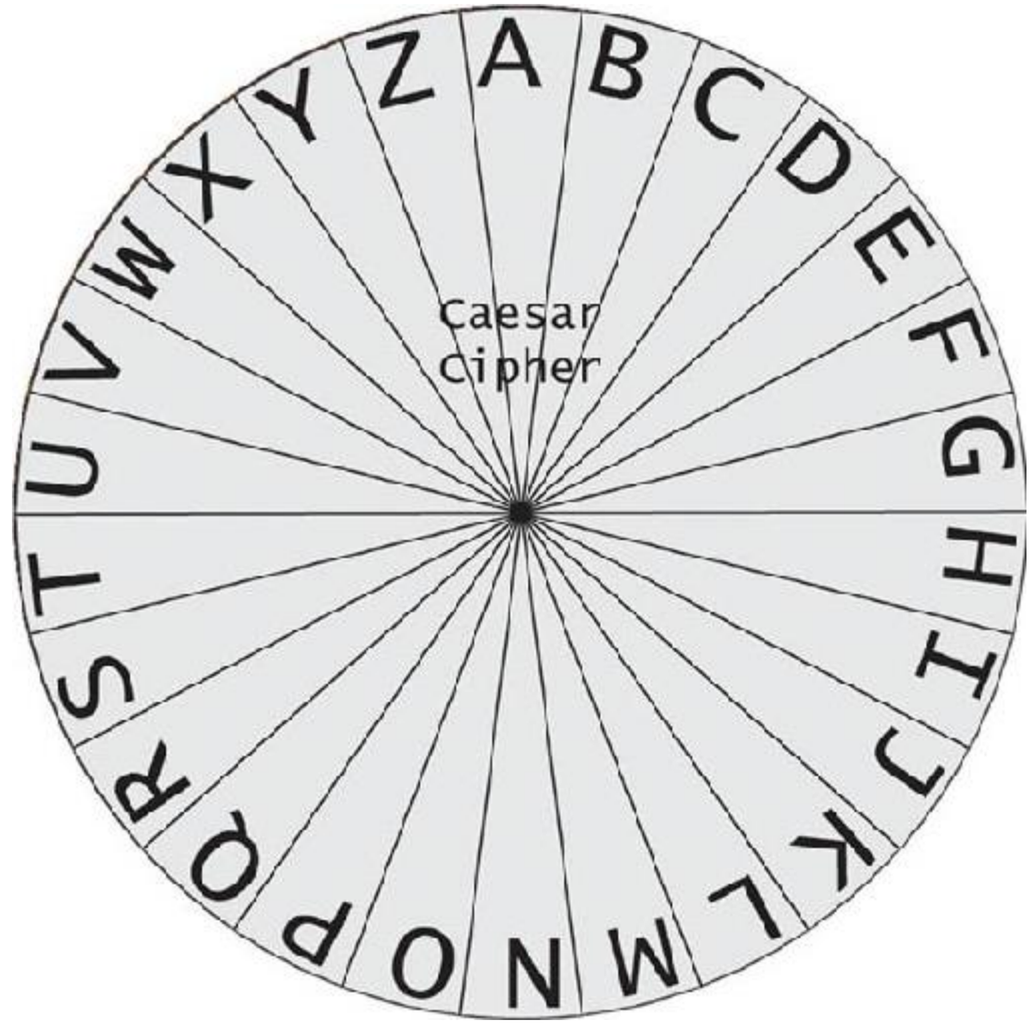
What are your thoughts about the Alberti Cipher?

Is it hard? Is it easy? Do you think it is secure? Or any other thoughts you have…

Use the post it notes to write any thoughts you have and post them below! We will use these as part of our discussion later.



Outer Cipher Wheel



Inner Cipher Wheel

Self-Checking Cards for practicing Alberti Cipher

This page contains the front of the cards and the next page will be printed on the back.

Directions Use your cipher wheel to decipher the ciphertext answers to the following jokes. Write the answers in your crypto-journal and then check them by turning the question card over to find the correct answer!
What is the clumsiest bee? Ll mfxmwtyr Qruu
Why can't you tell an egg a joke? Wep iecdp Jlajlt dy
What is more clever than a talking cat? Ss khwddafy Qruu

Self-Checking Cards for practicing Alberti Cipher

This page contains the back of the cards and the previous page will be printed on the front.

A bumbling bee

It might crack up

A spelling bee

Shhhh…It's A Secret: Learning the Key to Cryptography
Crypto-Practice for the Alberti Cipher

Below is an enciphered clue to the location of a hidden object in the room. Decipher the clue in the space provided by using your cipher wheel or the one you can find at the link on our session website. Write the plaintext of the clue in the space provided.

Enciphered Clue:
Sklmvwflk kal mhgf s Gingox gz yinuur

gtj cuxq Qqj edu ev jxuiu.

vydt Kdro yxo drkd sc kvv kvyxo; Fqttp nsxnij;

dtz bnqq knsi Mftq bdulq iuft qmeq.

Write the deciphered clue below.

Where do you think the object is hidden? (Write your plaintext answer below.)

Now encipher your guess to the location of the object using the Alberti cipher.

Directions
Alberti Cipher Station

1. Use the link on our session webpage to view the Alberti Cipher Prezi (The web address is http://prezi.com/u3cfwjb38slk/?utm_campaign=share&utm_medium=copy but you should be able to see it by clicking on "Alberti Cipher Prezi" on the session website.) Then use the link on our session webpage to view the Alberti Cipher video. (The web address is https://drive.google.com/file/d/0B8_Iy2-ce3qlbzJvREF2dGlmdTQ/edit?usp=sharing but you should be able to see it by clicking on the "Alberti Cipher Video" on the session website.)

2. Complete as many of the self-checking cards as you need to for practice. When you understand the cipher and believe you can correctly use it, you may move on to the Crypto-Practice sheet. You and your partner can work together to solve the riddles on the front of the cards and then check your solution with the correct answer located on the back of the card. If you do not get the right answer, see if you can figure out your mistake. If you need to, ask for help! Mrs. Tuttle is nearby to help! To decipher your jokes, use one of the cipher disks in the station.

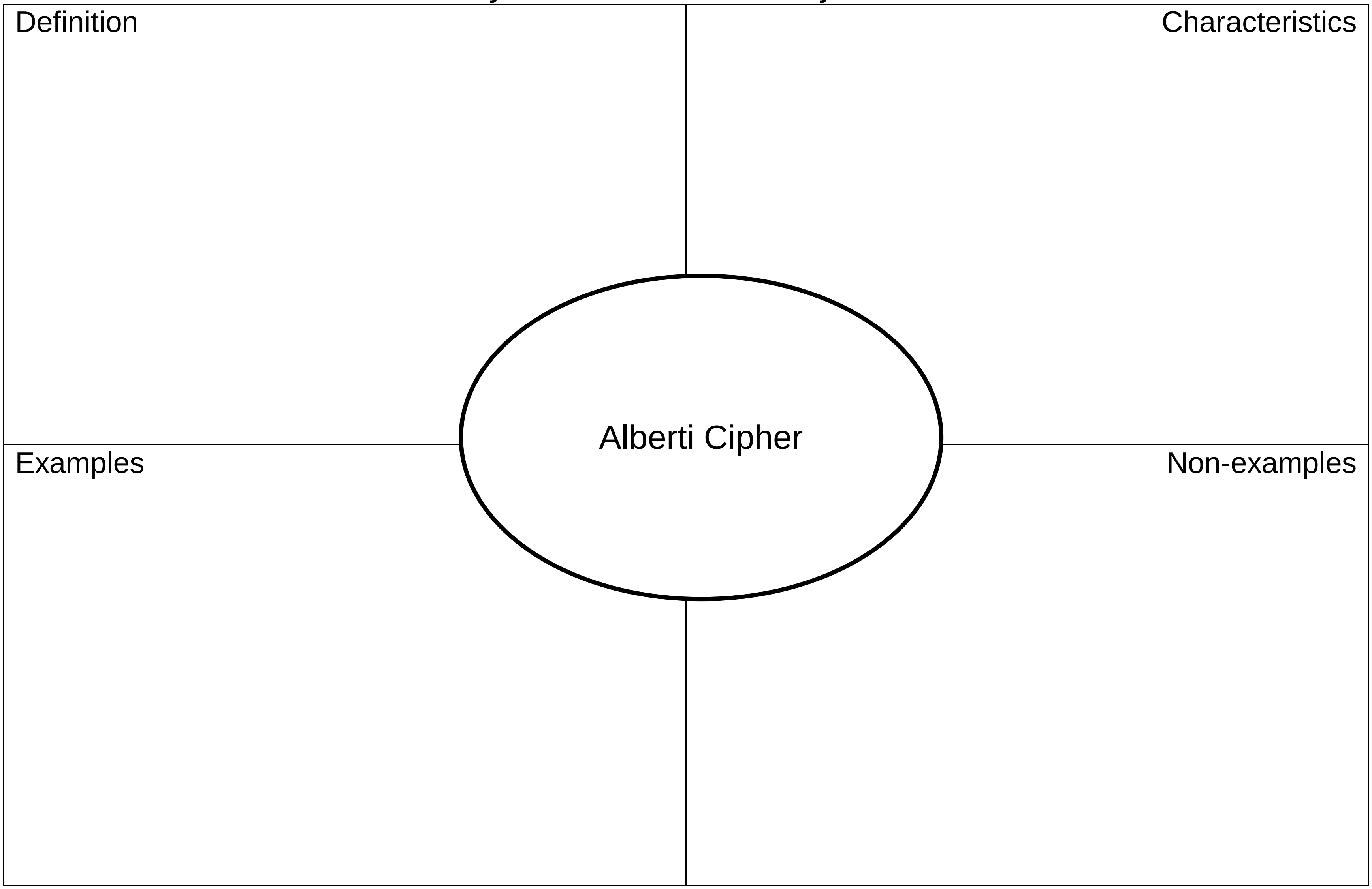
3. Use a cipher disk the Crypto-Practice Sheet in the station. The crypto-practice sheet will offer you a clue to the location of an object hidden in the room. Once you have deciphered the clue, write the plaintext for your guess about where the object is hidden. Then you will use your cipher disk to encipher your guess.

4. Complete your Frayer Model vocabulary sheet to explain your definition and understanding of the Alberti Cipher.

5. In your crypto-journal, write at least 2 positive aspects and 2 negative aspects of the Alberti Cipher.

6. Put your Crypto-practice form and your Frayer Model vocabulary sheet in the completed papers folder and move to the next station on your station card.

Frayer Method Vocabulary Sheet



Definition

Characteristics

Alberti Cipher

Examples

Non-examples

Vigenére Cipher

The following pages contain the pages/handouts/display sheets needed for the Vigenére Cipher Station. Below is a listing of what is included for this station. The pages that follow have this information in the following order.

- Pages for Display on the Vigenére Cipher Station Board

1. Vocabulary
2. Example of ciphertext and how to decipher
3. Picture of Vigenére Tableau
4. Did you know? Facts about Vigenére Ciphers
5. Student observation pages

- Vigenére Tableau

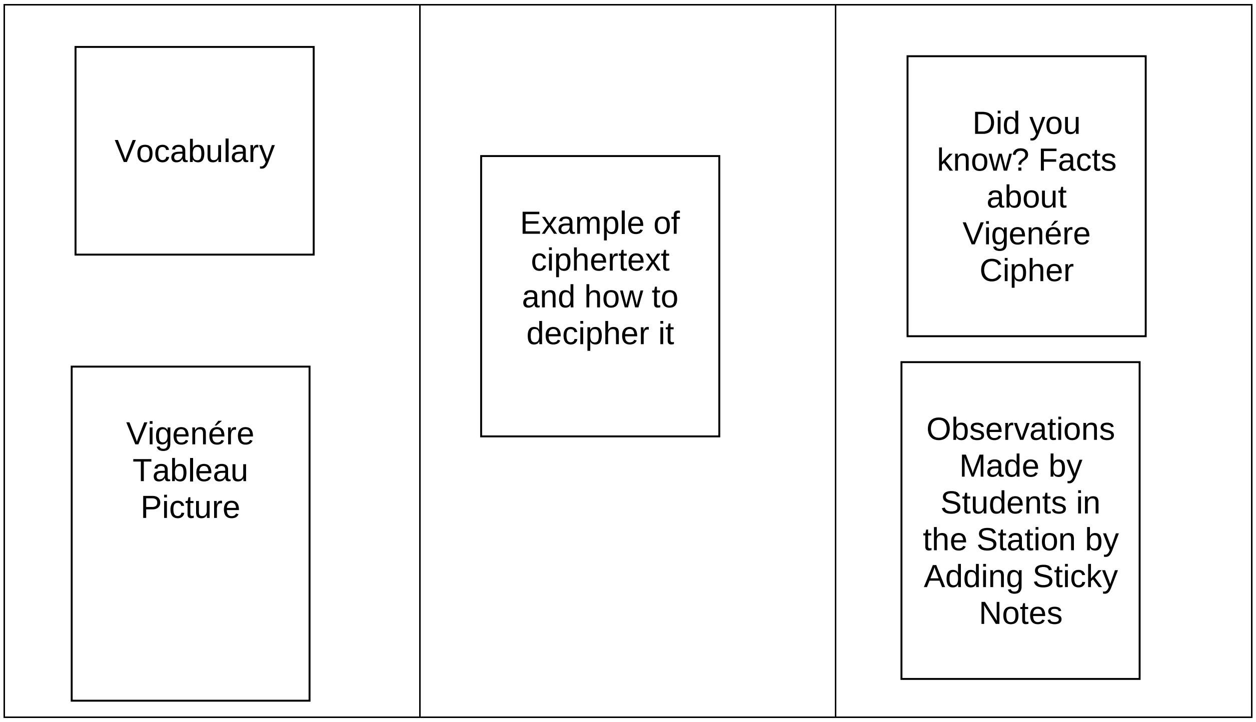
- Self-checking cards for practice with the Vigenére cipher

- Worksheet to complete at the Vigenére Cipher Station

- Student directions for the station

- Frayer Method Vocabulary Sheet

Layout of the Vigenére Cipher Station Board


Vocabulary
Vigenére Tableau Picture
Example of ciphertext and how to decipher it
Did you know? Facts about Vigenére Cipher
Observations Made by Students in the Station by Adding Sticky Notes

Vocabulary

Plaintext: text as it is normally written

Ciphertext: text that has been enciphered to prevent others from reading it

Cipher: A type of secret writing which replaces each letter in the plaintext with a different letter, number, or symbol

Polyalphabetic cipher: a cipher that uses different ciphertext symbols to represent a given plaintext letter within the same ciphertext message

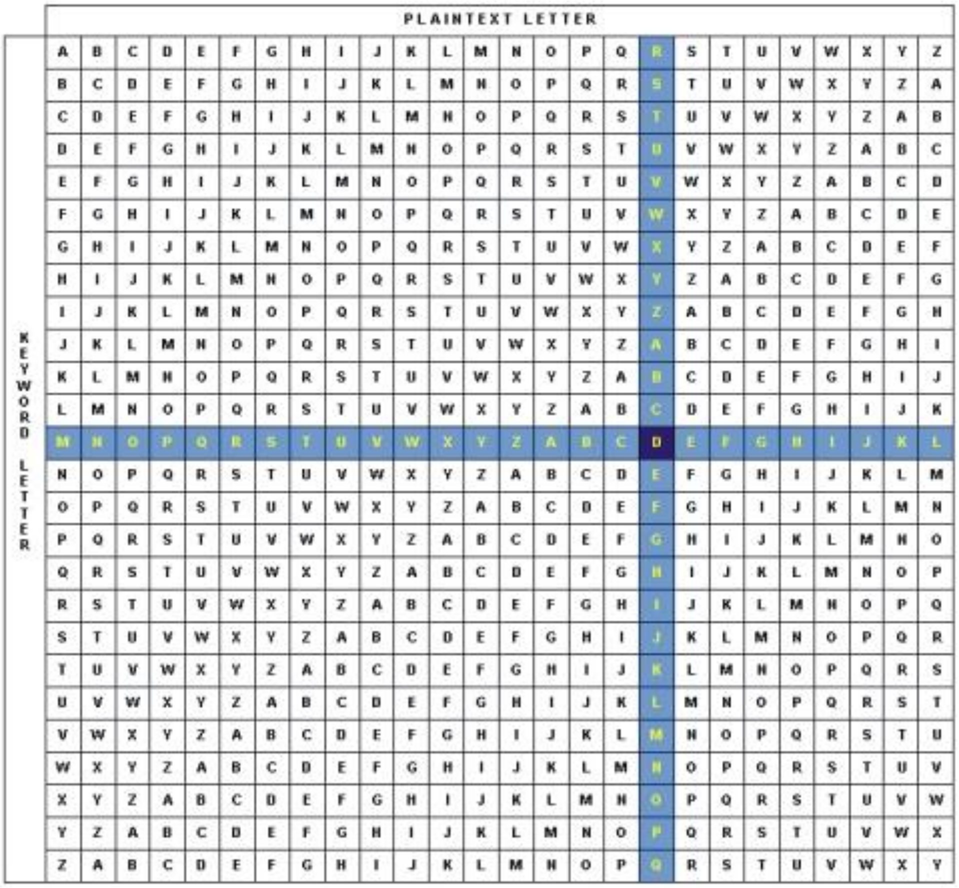
Vigenére Cipher: a type of polyalphabetic cipher which uses a key word and a Vigenére Tableau to encipher text

Algorithm: Mathematical formula or well-defined steps used to encipher text

Key: An important piece of information needed for the algorithm. In the Vigenére cipher, the key the word or phrase that indicates the order that the alphabets on the Vigenére tableau are used to encipher the message.

Example Using a Vigenére Cipher (Keyword: cryptography)

Our message is "Cracking a polyalphabetic cipher is harder than cracking a monoalphabetic cipher."



PLAINTEXT LETTER

KEYWORD LETTER

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

Plaintext	C	R	A	C	K	I	N	G	A	P	O	L	Y	A	L	P	H	A	B	E	T	I	C	C
Keyword	c	r	y	p	t	o	g	r	a	p	h	y	c	r	y	p	t	o	g	r	a	p	h	y
Ciphertext	E	I	Y	R	D	W	T	X	A	E	V	J	A	R	J	E	A	O	H	V	T	X	J	A

Plaintext	I	P	H	E	R	I	S	H	A	R	D	E	R	T	H	A	N	C	R	A	C	K	I
Keyword	c	r	y	p	t	o	g	r	a	p	h	y	c	r	y	p	t	o	g	r	a	p	h
Ciphertext	K	G	F	T	K	W	Y	Y	A	G	K	C	T	K	F	P	G	Q	X	R	C	Z	P

Plaintext	N	G	A	M	O	N	O	A	L	P	H	A	B	E	T	I	C	C	I	P	H	E	R
Keyword	y	c	r	y	p	t	o	g	r	a	p	h	y	c	r	y	p	t	o	g	r	a	p
Ciphertext	L	I	R	K	D	G	C	G	C	P	W	H	Z	G	K	G	R	V	W	V	Y	E	G

Vigenére Tableau

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

Did You Know?

- The Vigenére Cipher was created in 1586 by Blaise de Vigenére.

- Vigenére combined the works of Leon Battista Alberti and Johannes Trithemius

- Vigenére used the concept of changing the pairing of the ciphertext characters with the plaintext characters from Alberti

- Vigenére used the tableau created by Trithemius

- Vigenére improved the Alberti cipher by adding a keyword that defined how ciphertext characters were paired with plaintext characters.

What are your thoughts about the Vigenére Cipher?

Is it hard? Is it easy? Do you think it is secure? Or any other thoughts you have…

Use the post it notes to write any thoughts you have and post them below! We will use these as part of our discussion later.

Vigenére Tableau Form

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

Self-Checking Cards for practicing Vigenére Cipher

This page contains the front of the cards and the next page will be printed on the back.

Directions

Use your Vigenére Tableau to decipher the ciphertext answers to the following jokes. Write the answers in your crypto-journal and then check them by turning the question card over to find the correct answer!

What occurs once in every minute, twice in every moment, but never in a hundred thousand years?
(Keyword: Riddle)

kph opxkmu p

If I have it, I don't share it. If I share it, I don't have it. What is it?
(Keyword: Code)

c ghgtsw

What is so delicate that saying its name breaks it?
(Keyword: Code)

uwoipqh

Self-Checking Cards for practicing Vigenére Cipher

This page contains the back of the cards and the previous page will be printed on the front.

The letter M

A secret

Silence

Shhhh…It's A Secret: Learning the Key to Cryptography
Crypto-Practice for the Vigenére Cipher

Below is an enciphered clue to the location of a hidden object in the room. Decipher the clue in the space provided by using your cipher wheel or the one you can find at the link on our session website. Write the plaintext of the clue in the space provided.

Enciphered Clue (Keyword: cipher):
Yptu cfw nxywk czgpzv kv rseju,

gdb swvmc zmk cb dui fh ut.

P ed cta hpfpm, qbx cqwz prjklt

hru c xgpdv awj dmcn ajyica atl.

Write the deciphered clue below.

Where do you think the object is hidden? (Write your plaintext answer below.)

Now encipher your guess to the location of the object using the Vigenére cipher. Keyword: ____________________

Directions
Vigenére Cipher Station

1. Use the link on our session webpage to visit the Vigenére Cipher videos. View the first video by clicking on Vigenére Cipher Video 1 on our session webpage for today. Stop the video when the timer reads 3:08. Then watch the second video by clicking on Vigenére Cipher Video 2 on our session webpage for today. Watch this video until you believe that you understand how to encipher using the Vigenére Cipher. You will probably not need to watch the entire video to do this. (The web addresses for the videos are http://www.youtube.com/watch?v=K1SuiUu4kG0 and http://www.youtube.com/watch?v=9ZU5WHvYTGM but you should be able to see them by clicking on "Vigenére Cipher Video 1" and "Vigenére Cipher Video 2" on the session website.)

2. Use a Vigenére Tableau or the interactive one located at http://www.mathman.gr/component/content/article/10/639-cryptography-Vigenére-cipher.html to complete as many of the self-checking cards as you need to for practice. When you understand the cipher and believe you can correctly use it, you may move on to the Crypto-Practice sheet. You and your partner can work together to solve the riddles on the front of the cards and then check your solution with the correct answer located on the back of the card. If you do not get the right answer, see if you can figure out your mistake. If you need to, ask for help! Mrs. Tuttle is nearby to help! To decipher your jokes, use one of the cipher disks in the station.

3. Use a Vigenére Tableau or the interactive one located at http://www.mathman.gr/component/content/article/10/639-cryptography-Vigenére-cipher.html to complete the Crypto-Practice Sheet in the station. The crypto-practice sheet will offer you a clue to the location of an object hidden in the room. Once you have deciphered the clue, write the plaintext for your guess about where the object is hidden. Then you will use your cipher disk to encipher your guess.

4. Complete the Frayer Method sheet in the station by explaining the vocabulary word on it with your partner.

5. In your crypto-journal, write at least 2 positive aspects and 2 negative aspects of the Vigenére Cipher.

6. Put your Crypto-practice form and your Frayer method sheet in the completed papers folder and move to the next station on your station card.

Frayer Method Vocabulary Sheet

Definition

Characteristics

Vigenére Cipher

Examples

Non-examples

Rail Fence Cipher
Answer Key

R F E H
A L E C C P E
I N I R

Below is an enciphered clue to the identity of a hidden object in the room. Decipher the clue in the space provided by using the graph paper at your station. Write the plaintext of the clue in the space provided.

Enciphered clue: key = 3

WSEEHTINRNEAGSD

What signers need

Write the deciphered clue below.

What signers need

What do you think the object is? (Write your plaintext answer below)

Answers will vary.

Now encipher your guess as to the identity of the object using the graph paper provided. (Include the key and if you are using nulls in your guess)

Answers will vary, but the plaintext above should be correctly enciphered using the rail fence cipher and the key used for enciphering should be included.

Today, the hidden object is a pen.

Route Transposition Cipher

Below is an enciphered clue to the identity of a hidden object in the room. Decipher the clue in the space provided by using the graph paper at your station. Write the plaintext of the clue in the space provided.

Enciphered clue: key = 5 x 5 spiral grid

LXXXXOIPTXPRAWXTCSRXRETIX

A script writers tool

Write the deciphered clue below.

A script writers tool

What do you think the object is? (Write your plaintext answer below.)

Answers will vary.

Now encipher your guess as to the identity of the object using the graph paper provided. (Include the key in your guess)

Answers will vary, but the plaintext above should be correctly enciphered using the route cipher and the key used for enciphering should be included.

Today, the hidden object is a pen.

Shhhh…It's A Secret: Learning the Key to Cryptography
Crypto-Practice for the Alberti Cipher
Answer Key

Below is an enciphered clue to the location of a hidden object in the room. Decipher the clue in the space provided by using your cipher wheel or the one you can find at the link on our session website. Write the plaintext of the clue in the space provided.

Enciphered Clue:
Sklmvwflk kal mhgf s Gingox gz yinuur
Students sit upon a chair at school
gtj cuxq Qqj edu ev jxuiu.
and work at one of these.
vydt Kdro yxo drkd sc kvv kvyxo; Fqttp nsxnij;
Find the one that is all alone; look inside;
dtz bnqq knsi Mftq bdulq iuft qmeq.
and you will find the prize with ease.

Write the deciphered clue below.

Students sit upon a chair at school and work at one of these.
Find the one that is all alone; look inside; you will find the prize with ease.

Where do you think the object is hidden? (Write your plaintext answer below.)

Answers will vary.

Now encipher your guess to the location of the object using the Alberti cipher.

Answers will vary but they should encipher the plaintext above correctly using a cipher disk.

Today, the hidden object is in a student desk.

Shhhh…It's A Secret: Learning the Key to Cryptography
Crypto-Practice for the Vigenére Cipher
Answer Key

Below is an enciphered clue to the location of a hidden object in the room. Decipher the clue in the space provided by using your cipher wheel or the one you can find at the link on our session website. Write the plaintext of the clue in the space provided.

Enciphered Clue (Keyword: cipher):
Yptu cfw nxywk czgpzv kv rseju,
When you first arrive in class,
gdb swvmc zmk cb dui fh ut.
you often sit at one of me.
P ed cta hpfpm, qbx cqwz prjklt
I am all alone, but look inside
hru c xgpdv awj dmcn ajyica atl.
and a prize you will surely see.

Write the deciphered clue below.

When you first arrive in class, you often sit on one of me.
I am all alone, but look inside and a prize you will surely see.

Where do you think the object is hidden? (Write your plaintext answer below.)

Answers will vary.

Now encipher your guess to the location of the object using the Vigenére cipher. Keyword: ____________________

Answers will vary, but this should correctly encipher the plaintext above.

Today, the object is hidden in a student desk.

Assessment Rubrics (Day 2)

Station Assessments

	Did not attempt activity (0 pts.)	Partially completed the activity (1 pt.)	Completely finished the activity but contained more than 5 errors (2 pts.)	Completely finished the activity but the response contained 1-5 errors (3 pts.)	Completely finished the activity with no errors (4 pts.)
First Station Decipher Clue Activity					
First Station Encipher Guess Activity					
Second Station Decipher Clue Activity					
Second Station Encipher Guess Activity					
Total					/16

Positive and Negative Aspects Assessment

	Student did not attempt (0 pts.)	Student listed only one positive or one negative aspect (1 pt.)	Student listed only one positive and one negative aspect (2 pts.)	Student only listed 3 aspects instead of 4 (3 pts.)	Student listed 2 positive aspects and 2 negative aspects (4 pts.)
First Cryptosystem					
Second Cryptosystem					
Total					/8

LESSON #3
Cracking the Code

I. DEFINE OBJECTIVES AND CONTENT	
LESSON OBJECTIVE	Students will use frequency analysis to determine the plaintext of a message encrypted using a monoalphabetic cipher. Students will list the steps that can be used to break a polyalphabetic cipher.
POINT TO PONDER	A code is only as good as its key.
ESSENTIAL QUESTION	Does the **INTERACTION** between code makers (cryptographers) and code breakers (cryptanalysts) serve a good purpose or a bad one?

CONTENT Outline the content you will teach in this lesson.	9. Cryptanalysis A. The art of figuring out the secret meanings of messages B. The process of analyzing encrypted messages for patterns in order to determine the key and "break" a cryptosystem C. Creates a competition or "game" between cryptographers and cryptanalysts D. Interacts with cryptography in a way that causes a constant cycle of change 1. A cryptosystem is broken using cryptanalysis 2. Cryptographers create a stronger and more secure cryptosystem 3. Cryptanalysts use more advanced techniques to break the new cryptosystem and the cycle continues E. Frequency analysis 1. First used by the fifteenth century Egyptian cryptologist, Shihab al-Qalqashandi 2. Involves the analysis of words or symbols representing words to find patterns in codes 3. Involves the analysis of the number of times each symbol or letter appears in a given example of ciphertext in monoalphabetic ciphers 4. Cannot be applied to short examples of codes and ciphers since there will not be enough data 5. Can be used on data collected from multiple examples of short ciphertext if the key is used multiple times 6. Frequencies of letters vary based on the language of the plaintext used in the cipher F. Polyalphabetic Ciphers 1. In 1854, Cambridge mathematics professor Charles Babbage reasoned that if the key was short and the text was long the key length could be determined for a Vigenére cipher and the cipher could be broken 2. Involves the analysis of text to find repeating patterns in the letters, symbols, and numbers in the ciphertext 3. The distances between these repeating patterns helps determine the key length

4. Once the key length is known, the ciphertext becomes multiple examples of monoalphabetic ciphers that are susceptible to frequency analysis.

G. "Hacking" techniques

1. Determine a vulnerability in a system so that enough data can be gathered to determine the key
2. BEAST Exploit to crack web encryption
    a) Uses suspicious links or malicious websites to infect a computer
    b) Uses malicious program to monitor data exchanged between the computer and secure websites
    c) Program inserts blocks of plaintext and attempts to decrypt those blocks by guessing the encryption key
    d) Program gathers enough data to correctly find the key and uses it to reverse engineer the key and decrypt confidential data stored on the computer
3. One-time pad
    a) Uses an infinite number of unique keys that are as long as or longer than the plaintext so that there are no repeating patterns in the ciphertext
    b) Advantages
        (1) Theoretically unbreakable
        (2) Most secure cipher system
    c) Disadvantages
        (1) Key must be as long or longer than the text that is being encrypted
        (2) Key can only be used once
        (3) If the key is accidentally used more than once, data can be gathered and frequency analysis is possible
        (4) Unlimited number of keys are necessary

II. PRE-PLANNING	
What will students UNDERSTAND as	

a result of this lesson? How does this connect to the Essential Question?	Students will be able to understand that given enough time almost all cryptosystems can be "broken" or "cracked." Students will understand how the steps used to break simple, classical ciphers (Shift Ciphers and Vigenére Ciphers) can be applied to more complex ciphers used today by computers. Students will understand the roles cryptanalysts and cryptographers play in their on-going competition between code making and code breaking. These understandings will help students see how cryptanalysts work and the **INTERACTION** between cryptanalysts and cryptographers. Experiencing this **INTERACTION**, students will be able to create their own opinion about whether this **INTERACTION** serves a positive or negative purpose.
What will students be able to DO as a result of this lesson?	Students will be able to "crack" a monoalphabetic cipher by using frequency analysis. Students will be able to explain the steps a cryptanalyst can use to "break" or "crack" a polyalphabetic cipher with a short encryption key.

III. PLANNING	
HOOK Describe how you will grab students' attention at the beginning of the lesson. BE CREATIVE.	TIME: 5 min Provide students with cards as they enter the classroom that contain two ciphers. Inform the students that we have intercepted information from the Grizzlies from D.F. Walker Elementary School. We think that they may be performing recognizance about our activities and may know what we are working on for our "client" team. We must decipher the information to know what they know! Allow students 5 minutes to study the code and determine what they think we should do to decipher it…they can also use this time to attempt to decipher the ciphers. (See attached sheet for ciphers) After students have analyzed the text provided in the hook, we will discuss the ideas students came up with to be able to decipher the texts.
INSTRUCTION Explain Step-by-step what you will do in this lesson. Be explicit about ties to Points to Ponder, Essential Question, and Interactions here. Include ALL support and teaching materials with your unit.	TIME: 60 min 1. We will return the crypto-journals to the students. 2. We will provide students with an example of plaintext and have them share ideas about what they notice about the characteristics of the text (see attached). Examples of characteristics they may notice are the fact that the letter E (in English) shows up the most times, that there are repeating patterns of letters, that there are several two and three letter words that repeat, etc. 3. Once these ideas are shared, we will begin a discussion about how cryptanalysts look for these patterns that they know exist in each language in order to break a monoalphabetic cipher. 4. Using the tool located online at http://rumkin.com/tools/cipher/frequency.php we will display a frequency analysis graph using this example text (from step 2) so that students can see the relative frequencies of each of the letters in the text. We will discuss whether they believe that this pattern would fit typical English text. 5. As a group, we will view the video located at https://www.khanacademy.org/math/applied-math/cryptography/crypt/v/caesar-cipher (2:37). 6. Students will be provided with a frequency table listing the letters of the English alphabet in the order of the frequency they occur. They will also be given a list of the most often used two and three letter words (listed in the order of their frequency of occurrence in ordinary English speech).

7. The students will then look back at the first example of text that was intercepted as part of the hook. They will use the frequency analysis tool located at http://rumkin.com/tools/cipher/frequency.php to determine the relative frequencies of the letters in the ciphertext.
8. Using the list of English letter and word frequencies and logic, students, with a partner, will try to decipher the text using the frequency analysis graph. Teachers will circulate to help students apply the frequency information to the text (if this help is needed). (For example, the letter that occurs most often in the ciphertext probably represents the letter e in English, etc. Students will have to combine logic with the frequency table, though. For example, once they have figured out a few letters, they can use their knowledge of English words to determine the letters still missing from a given word. They will also use logical thinking such as T is not a one letter word in English, etc.)
9. As a class, we will share the plaintext we all deciphered from the first intercepted text from the hook.
10. As a class, we will put the text of the second intercepted message from the hook into the frequency analysis tool. Students will see that this message (which, unknown yet to the students, is polyalphabetic) does not match the anticipated frequencies. (The bars on the graph that results from this ciphertext shows several letters that occur at a very high frequency level. In a monoalphabetic cipher, they cannot all be "e" and the frequency analysis of English shows that other letters should not occur as frequently as "e" does in the English language.) The teachers will lead the students to determine that the ciphertext must use a polyalphabetic cipher.
11. We will display (as an example) our same example text from step 3 enciphered using a Vigenére Cipher with HI as our keyword (see attached). We will compare the plaintext and ciphertext and notice where cipher letters repeat as the short key repeats (see teacher notes sheet that is attached).
12. We will provide the students with a worksheet to use to help decipher the second intercepted text from the hook (see attached).
    a. At the bottom of the worksheet is a table with groups of letters listed that repeat in the ciphertext. With a partner, students will be assigned a set of letters that they will find in the text. They will locate and underline each occurrence of the letter string in the ciphertext.

	b. Student pairs will then go to the SmartBoard to underline the letters that they found repeating in the text. Each pair will use a different color so that we can differentiate the groups that go together. c. After the teachers model the process with students using the rri letter series, students will count the number of letters located between the end of one of the strings of repeated letters and the last letter in the next occurrence. They will record this information in the appropriate spaces on the table on the worksheet (see attached worksheet). In the rri example, we will count the letters starting with the first one after the i and count the i in the next rri occurrence as the final letter. d. After a brief discussion about the prime factorization of the first number (the one the teachers found) and a demonstration of how to find the prime factors of that first number, students will work with their partners to find the prime factors of each of the numbers they found and added to our collective table. Each pair will then add these prime factors to the table (see attached sheet). e. Using this information, we will make an educated guess as to the length of the key word used in the cipher and discuss how this information would create multiple monoalphabetic ciphers that could be broken using frequency analysis. We would then discuss the time it would take to complete this process. Students will be free to attempt to break this cipher at home since the process would take a long time. 13. We will also discuss how computer programs can be (and have been) created to complete this process more quickly. As an example, remind the students that they were able to use the online frequency tool in this lesson to find the frequencies of the letters in the ciphertext—a job that prior to the computer age would have had to be completed by hand. In this way, technology has interacted with cryptography to cause cryptographers to use different techniques that could not be cracked as quickly by a computer as these classical systems could. We will use this as a spring board to discuss the point to ponder…A code is only as good as its key. After using these steps to break a cipher, students should be able to explain the importance of a key and discuss their views on this point to ponder. Refer also to the essential question…What are

your views now about whether the **INTERACTION** between code makers and code breakers is positive or negative? We will use this time to also focus on the camp theme of **INTERACTION**—the **INTERACTION** between technology and cryptography and the **INTERACTION** between code makers and code breakers.

14. However, the idea of looking for patterns and guessing the key are techniques used by hackers of today's systems, too. We will briefly explain how the BEAST exploit was used to allow a program to decipher confidential communication from a secure source (see content outline).
15. Ask students what we were able to do to get a clue to the key length of the polyalphabetic cipher we used today. (We looked for patterns in the ciphertext so that we could make an educated guess about the length of the key word since the letters in the word would have to repeat to form the repeating patterns in the ciphertext.) Ask the students what would happen if there were no repetitions. Could a cryptanalyst use the technique we used to break a cipher with no repeating patterns? Do you think there would be another strategy he or she could use? What "clues" could a cryptanalyst look for in that type of cipher? Present students with the idea of a one-time pad (see content outline). Explain to students that this is the only universally secure cryptosystem (in theory). If the key is as long as or longer than the text, we would not be able to find any repeating patterns in order to use monoalphabetic frequency analysis to break the cipher. However, if the key is used more than once, we can eventually gather enough data. Have students share what they would see as drawbacks to this system. Ideas shared could include the need for an infinite number of keys, the need to make sure the sender and receiver are using the same key each time, the fact that accidentally reusing a key could provide data needed to perform frequency analysis, and the keys would have to be recorded somewhere because they are so long—an action which would expose them to the possibility of being lost or stolen. Refer to the point to ponder again. What are any new thoughts about the statement?
16. Students can visit our class padlet for today and their crypto-journal to add any information they think will be important to remember and incorporate into the cryptosystem they are creating.
17. After reviewing their notes, students will discuss, with their cryptosystem creation partner, the ideas they want to use

	in their cryptosystem. The student pairs can share their ideas on today's padlet so that everyone can benefit from their thoughts and so that others in the group might be able to correct misunderstandings. 18. We will distribute copies of the final project rubric to the students. We will discuss the rubric and the specific expectations for the project (see attached rubric). We will tell the students that today they should focus on discussing their new cryptosystem and creating it with their cryptosystem creation partner. We will tell the students that tomorrow we will discuss and demonstrate how to create the instructional video part of the project. 19. In the students' crypto-journals, they will find a cryptosystem creation form (see attached crypto-journal pages). We will have the students look at these pages of the crypto-journal and discuss the expectations for each part as well as how the cryptosystem creation form fits with the rubric for the project. On this form, the students will organize their ideas for their cryptosystem and their final product. Students will work with their partner to create their cryptosystem and write the reasons they believe their cryptosystem would be secure (or secure enough for the purposes of our project). This information will be filled in on the cryptosystem creation project form. Students will use the remaining time to work on creating their cryptosystem and their final product.
ASSESSMENT (Performance Task) What will the students DO to demonstrate that they have mastered the content? Be specific and include actual assessment with unit materials.	TIME: 5 min Students will be provided with a short example of monoalphabetic text to decipher. We will tell the students that the key for the text had been used before so we have already made a frequency graph they can use. Students will use the frequency graph to decipher the short text (see attached). As a ticket out the door, students will briefly write the steps that would need to be used to break a polyalphabetic cipher on an index card we will provide. Students will submit this index card as they leave the room for their next activity on their schedule.

DOES THE ASSESSMENT ALLOW YOU TO DETERMINE WHETHER OR NOT THE STUDENTS HAVE MET YOUR STATED LESSON OBJECTIVE? [✓ YES] OR NO

ASSESSMENT AND INSTRUCTIONAL MATERIALS

Insert ALL materials here including Assessments and Instructional Materials. Explicitly LIST any additional files for this lesson. Be sure that ALL materials have been submitted for this lesson.

Files and links needed for this lesson:
(All of these links are located on our session website. They are also listed in the lesson plan at the appropriate places.)

Frequency Tool
http://rumkin.com/tools/cipher/frequency.php

Caesar Cipher Video
https://www.khanacademy.org/math/applied-math/cryptography/crypt/v/caesar-cipher

Padlet for Day 3
http://padlet.com/wall/3cq7g0g1od

Attachments for Day 3:

Intercepted Messages

1. Hp slgp tyepcnpaepo dzxp nzxxfytnletzy esle dszhd esp Mwlnvslhvd lcp rztyr ez mp fdtyr l yph nzop hspy esp rlxpd mprty lrlty! Espcp htww mp yz hlj qzc fd ez fyopcdelyo hsle espj lcp dljtyr tq hp oz yze qtrfcp zfe esp vtyo zq djdepx espj htww mp fdtyr. Hp xfde nzxp fa htes l awly ez qtrfcp zfe esptc nzop!

2. Iss kvc bmerx! Uo rcoh ry jgxh mex urer dlc msbo sp mmnrip sw rrer dlci agvp zo yqsre! Dlc Lpymofkai diyw qcwfcbw qevc kvc dvgmow! S xfsri dlci lyfi ycocn el yyr-yj-ryal qvmet ry lcvt, zex G nsl'd xfsri dlyd xfoc fkzc biaomtoh rri ayhc yv astfov wox! Uo wrspj reto xgwi! Uril dlci vcmigfi rri ayhc gi uspj kpqy rcoh ry fc dlcbi! Akr yxcmxi dsrb yyr glcbi rri Zveaulygoq kvc xsu cs rrer gi akr dypjya rrik krb pmln ssd afor rriw gmjv vcmigfi rri ayhc?

Text used in Step 2

Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper.

The development of cryptography has been paralleled by the development of cryptanalysis — the "breaking" of codes and ciphers. The discovery and application, early on, of frequency analysis to the reading of encrypted communications has, on occasion, altered the course of history. Thus the Zimmermann Telegram triggered the United States' entry into World War I; and Allied reading of Nazi Germany's ciphers shortened World War II, in some evaluations by as much as two years.

Until the 1970s, secure cryptography was largely the preserve of governments. Two events have since brought it squarely into the public domain: the creation of a public encryption standard (DES), and the invention of public-key cryptography.

In cryptanalysis, *frequency analysis* is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.

Relative Frequencies in English

Below is a table that shows the relative frequencies of letters and words in the English language. The most common letters or words are listed at the top.

Frequency order	Letters	Double letters	2 letter words	3 letter words	4 letter words
1	E	ss	of	the	that
2	T	ee	to	and	with
3	A	tt	in	for	have
4	O	ff	it	are	this
5	I	ll	is	but	will
6	N	mm	be	not	your
7	S	oo	as	you	from
8	H		at	all	they
9	R		so	any	know
10	D		we	can	want
11	L		he	had	been
12	C		by	her	good
13	U		or	was	much
14	M		on	one	some
15	W		do	our	time
16	F		if	out	
17	G		me	day	
18	Y		my	get	
19	P		up	has	
20	B		an	him	
21	V		go	his	
22	K		no	how	
23	J		us	man	
24	Q		am	new	
25	X			now	
26	Z			old	

Text from lesson plan step 2 enciphered using a Vigenére Cipher with the keyword Hi

Jzfxawnzhxog, apl czm vn jwkmz iul jqwplzz bv xywamjb zmjzlbz, jlohv apvcziulz wm gliya hov. Cubpt ymjmub kmjikmz, qa pha imlv apl aawyg vn dphb tqnpa jl khtsmk ksizapk jzfxawnzhxog — aphb pa, vn tmapvlz wm mukygwbpwu boia czm wmu iul wiwmy, wy xlzoiwa zqtxsm tmjphvpkht hqka. Pv apl mhzsg 20ap jmubbzf, bom pvcmubpwu wm kvuwtlf tmjphvpkht hvk msmjbywtmjphvpkht tijppvla, zcjp ha apl Muqnuh zvbvz tijppvl, xywcqkmk uvzl avxoqzbpkhbll hvk mmnpkpmub tmhvz wm mukygwbpwu; iul apl abjzmxclva qubywkcjbpwu wm msmjbywuqja hvk kvuwcaquo oiz istvell lthjvzhbl ajplula vn zbpts oymhblz jwtxsmeqag, twzb vn dppko iym lvaqymsg bvzcpbll aw wmu iul wiwmy.

Bom kmcmswwulva wm kygwbvoyiwpf pha imlv wiyistltll ig apl lldltvxtmub vn jzfxaiuisgzqz — bom "izlirquo" vn jwkmz iul jqwplzz. Bom kqzkvdlzf iul hxwtpkhbpwu, mhzsg vv, vn mzlybmukf iuisgzqz bv bom ymhlpvn wm mukygwbll jwtubvpkhbpwua oiz, wu wjkhapwu, isblzll apl kvcyal wm ppaawyg. Apba apl Hputmyuhvu Bltloyit byqnolzll apl Cuqamk Aaiamz' mubyg pvaw Dwytk Ehz P; iul Htsqll ymhlpvn wm Vhhp Olztiug'z kpxomya zpvzamumk Evzsl Diy QP, qu avul mcischbpwua ig ha tcjp ha aev gliya.

Bvaqs bom 1970z, alkbzl kygwbvoyiwpf eha siyoltf bom wzlalzcm vn nwcmyvtmubz.

Bdw ldlvaa oicm zqukl jywboob pb zybiymsg pvaw apl xbjsqj lvuhqu: bom jzliaqvv vn h xbjsqj mukygwbpwu aaiulhzk (LLA), hvk bom pvcmubpwu wm xbjsqj-slg jzfxawnzhxog.

Pv jzfxaiuisgzqz, nymxclvjg hvhtfapa pa apl aackg vn apl nymxclvjg vn smablzz wy oywbxz wm tlbamya pv h kpxomyblfa. Bom tmapvl pa ball ha hv hqk bv jymhspvn ksizapkht jqwplzz.

Teacher Notes Sheet

Repeated groups of letters that students can be guided to find are highlighted below.

Text used in Step 2

Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper.

The development of cryptography has been paralleled by the development of cryptanalysis — the "breaking" of codes and ciphers. The discovery and application, early on, of frequency analysis to the reading of encrypted communications has, on occasion, altered the course of history. Thus the Zimmermann Telegram triggered the United States' entry into World War I; and Allied reading of Nazi Germany's ciphers shortened World War II, in some evaluations by as much as two years.

Until the 1970s, secure cryptography was largely the preserve of governments. Two events have since brought it squarely into the public domain: the creation of a public encryption standard (DES), and the invention of public-key cryptography.

In cryptanalysis, *frequency analysis* is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.

Text above enciphered with a Vigenére Cipher with the keyword Hi

Jzfxawnzhxog, apl czm vn jwkmz iul jqwplzz bv xywamjb zmjzlbz, jlohv apvcziulz wm gliya hov. Cubpt ymjmub kmjikmz, qa pha imlv apl aawyg vn dphb tqnpa jl khtsmk ksizapk jzfxawnzhxog — aphb pa, vn tmapvlz wm mukygwbpwu boia czm wmu iul wiwmy, wy xlzoiwa zqtxsm tmjphvpkht hqka. Pv apl mhzsg 20ap jmubbzf, bom pvcmubpwu wm kvuwtlf tmjphvpkht hvk msmjbywtmjphvpkht tijppvla, zcjp ha apl Muqnuh zvbvz tijppvl, xywcqkmk uvzl avxoqzbpkhbll hvk mmnpkpmub tmhvz wm mukygwbpwu; iul apl abjzmxclva qubywkcjbpwu wm msmjbywuqja hvk kvuwcaquo oiz istvell lthjvzhbl ajplula vn zbpts oymhblz jwtxsmeqag, twzb vn dppko iym lvaqymsg bvzcpbll aw wmu iul wiwmy.

Bom kmcmswwulva wm kygwbvoyiwpf pha imlv wiyistltll ig apl lldltvxtmub vn jzfxaiuisgzqz — bom "izlirquo" vn jwkmz iul jqwplzz. Bom kqzkvdlzf iul hxwtpkhbpwu, mhzsg vv, vn mzlybmukf iuisgzqz bv bom ymhlpvn wm mukygwbll jwtubvpkhbpwua oiz, wu wjkhapwu, isblzll apl kvcyal wm ppaawyg. Apba apl Hputmyuhvu Bltloyit byqnolzll apl Cuqamk Aaiamz' mubyg pvaw Dwytk Ehz P; iul Htsqll ymhlpvn wm Vhhp Olztiug'z kpxomya zpvzamumk Evzsl Diy QP, qu avul mcischbpwua ig ha tcjp ha aev gliya.

Bvaqs bom 1970z, alkbzl kygwbvoyiwpf eha siyoltf bom wzlalzcm vn nwcmyvtmubz. Bdw ldlvaa oicm zqukl jywboob pb zybiymsg pvaw apl xbjsqj lvuhqu: bom jzliaqvv vn h xbjsqj mukygwbpwu aaiulhzk (LLA), hvk bom pvcmubpwu wm xbjsqj-slg jzfxawnzhxog.

Pv jzfxaiuisgzqz, nymxclvjg hvhtfapa pa apl aackg vn apl nymxclvjg vn smablzz wy oywbxz wm tlbamya pv h kpxomyblfa. Bom tmapvl pa ball ha hv hqk bv jymhspvn ksizapkht jqwplzz.

Cipher worksheet for Message #2

Iss kvc bmerx! Uo rcoh ry jgxh mex urer dlc msbo sp mmnrip sw rrer dlci agvp zo yqsre! Dlc Lpymofkai diyw qcwfcbw qevc kvc dvgmow! S xfsri dlci lyfi ycocn el yyr-yj-ryal qvmet ry lcvt, zex G nsl'd xfsri dlyd xfoc fkzc biaomtoh rri ayhc yv astfov wox! Uo wrspj reto xgwi! Uril dlci vcmigfi rri ayhc gi uspj kpqy rcoh ry fc dlcbi! Akr yxcmxi dsrb yyr glcbi rri Zveaulygoq kvc xsu cs rrer gi akr dypjya rrik krb pmln ssd afor rriw gmjv vcmigfi rri ayhc?

You will be assigned a string of letters from the chart below to find in the message above. Underline your assigned letters in the text above each time they occur.

Letter group	Number of occurrences	Distance between the occurrences (Count the letters between one letter in your assigned letter string and the next time that letter occurs in your letter string like your instructors demonstrated in class.)	Prime Factors of the distance between the occurrences
rri	6		
kvc	3		
		195	3 x 5 x 13
uo	2	183	3 x 61
dlc	3		
		183	3 x 61
xfsri	2		
dlci	3	105	3 x 5 x 7
ayhc	3		
		120	2 x 2 x 2 x 3 x 5

Cipher worksheet for Message #2

Answer Key

Iss kvc bmerx! Uo rcoh ry jgxh mex urer dlc msbo sp mmnrip sw rrer dlci agvp zo yqsre! Dlc Lpymofkai diyw qcwfcbw qevc kvc dvgmow! S xfsri dlci lyfi ycocn el yyr-yj- ryal qvmet ry lcvt, zex G nsl'd xfsri dlyd xfoc fkzc biaomtoh rri ayhc yv astfov wox! Uo wrspj reto xgwi! Uril dlci vcmigfi rri ayhc gi uspj kpqy rcoh ry fc dlcbi! Akr yxcmxi dsrb yyr glcbi rri Zveaulygoq kvc xsu cs rrer gi akr dypjya rrik krb pmln ssd afor rriw gmjv vcmigfi rri ayhc?

You will be assigned a string of letters from the chart below to find in the message above. Underline your assigned letters in the text above each time they occur.

Letter group	Number of occurrences	Distance between the occurrences (Count the letters between one letter in your assigned letter string and the next time that letter occurs in your letter string like your instructors demonstrated in class.)	Prime Factors of the distance between the occurrences
rri	6	48	2 x 2 x 2 x 2 x 3
		51	3 x 17
		36	2 x 2 x 3 x 3
		18	2 x 3 x 3
		15	3 x 5
kvc	3	90	2 x 3 x 3 x 5
		195	3 x 5 x 13
uo	2	183	3 x 61
dlc	3	36	2 x 2 x 3 x 3
		183	3 x 61
xfsri	2	48	2 x 2 x 2 x 2 x 3
dlci	3	57	3 x 19
		105	3 x 5 x 7
ayhc	3	48	2 x 2 x 2 x 2 x 3
		120	2 x 2 x 2 x 3 x 5

Message color coded by letters in the keyword

Iss kvc bmerx! Uo rcoh ry jgxh mex urer dlc msbo sp mmnrip sw rrer dlci

agvp zo yqsre! Dlc Lpymofkai diyw qcwfcbw qevc kvc dvgmow! S xfsri dlci

lyfi ycocn el yyr-yj-ryal qvmet ry lcvt, zex G nsl'd xfsri dlyd xfoc fkzc

biaomtoh rri ayhc yv astfov wox! Uo wrspj reto xgwi! Uril dlci vcmigfi rri

ayhc gi uspj kpqy rcoh ry fc dlcbi! Akr yxcmxi dsrb yyr glcbi rri Zveaulygoq

kvc xsu cs rrer gi akr dypjya rrik krb pmln ssd afor rriw gmjv vcmigfi rri

ayhc?

When you know that the distances between the repeated characters have a common factor of 3, you can guess that the keyword must be three characters long. Then, the message becomes 3 shift ciphers that can be solved using frequency analysis (as long as you have a message long enough for the analysis). Below are the letters that would be used in the frequency analysis of each of the shift ciphers:

Shift 1:
ikbrooyxerdmomrsrdivosdlmkdwwbekdmssdifcnyyyqeyvendsddokbooryyso
oosrowrdimfrygskyoydbkxxsygbrvugkxcrgkyyrkpndorgvmfry

Shift 2:
Svmxrhjhxelssmiwelapyrlpoaiqfwvvvoxrllioeyjavtltxsxrlxczimhihvtvxwpexiilvi
iihipqrhflirciryliielovsseirpairmsarimviiih

Shift 3:
sceucrgmurcbpnprrcgzqecyfiyccqccgwficyyclrrlmrczglfiyffcatracafwurjtgulcc
gracujqcrccaymdbrcrzayqcurradjrkblsfrwjcgrac

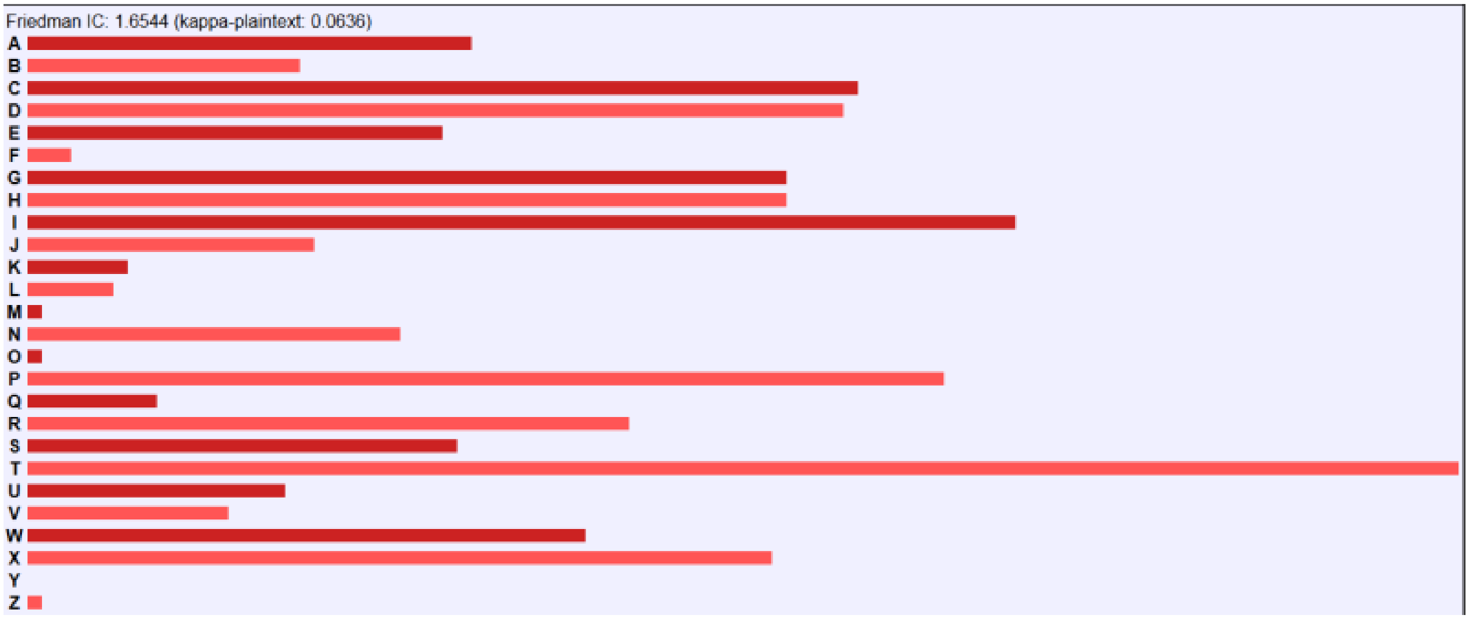
Plaintext for the Intercepted Messages
Answer Key

1. We have intercepted some communication that shows the Blackhawks are going to be using a new code when the games begin again! There will be no way for us to understand what they are saying if we do not figure out the kind of system they will be using. We must come up with a play to figure out their code!

2. You are right! We need to find out what the code or cipher is that they will be using! The Blackhawk team members sure are tricky! I think they have asked an out-of-town group to help, but I don't think that they have received the code or cipher yet! We still have time! When they receive the code we will also need to be there! Can anyone find out where the Blackhawks are now so that we can follow them and find out when they will receive the code?

Show What You Know
Assessment

1. We have intercepted one last message from the Grizzlies. We know that they used the same key they have used before. We have used the data from previous messages to make the frequency graph below. Use the frequency graph and your knowledge of the relative frequencies of letters and words in English to decipher this message.



Lt ctts iwpi itpb'h htrgti

Crypto-Journal Pages for the

Cryptosystem Creation Form

What is the name of your new cryptosystem?

Did you use any aspects of the cryptosystems we learned this week? If so, which one(s)?

List at least 3 aspects of your cryptosystem that you think makes it secure (or at least secure enough for the purposes of this project).

1.

2.

3.

Explain how your cryptosystem works.

Provide at least one example using your cryptosystem.

Plan your video instruction here and on the back of this page.

Assessment Answer Key and Rubric

1. The message says “We need that team’s secret.”
   Rubric:
   0 pts. Did not attempt problem
   1 pt. Correctly filled in at least 6 letters.
   2 pts. Correctly filled in at least 10 letters.
   3 pts. Correctly filled in at least 14 letters.
   4 pts. Correctly filled in all letters.

2. List the steps to “cracking” a Vigenére Cipher on an index card.
   a. Find repeated strings of letters in the ciphertext.
   b. Count the spaces between the occurrences of the repeated strings.
   c. Find the prime factors of the numbers of spaces between the occurrences of the repeated strings.
   d. Find the common factor of all of the numbers of spaces between the occurrences of repeated strings.
   e. Guess the key length based on the common factor.
   f. Break the cipher into several monoalphabetic ciphers.
   g. Use frequency analysis and reasoning to break the monoalphabetic ciphers.

Rubric: **Note: Students may have more or less steps than are listed above, but the information above should be included in some way in the students’ steps.

0 pts. Did not attempt question
1 pt. Included at least 2 of the steps above.
2 pts. Included at least 4 of the steps above.
3 pts. Included at least 6 of the steps above.
4 pts. Included all steps above

3 points on each section would demonstrate acceptable understanding for this assessment.

Rubric for Final Project (All of the following aspects should be evident in the video the students create.)

	Level 1 Novice 0 pts.	Level 2 Developing 2 pts.	Level 3 Acceptable 4 pts.	Level 4 Outstanding 6 pts.
The student created a new cryptosystem.	No cryptosystem is presented or the cryptosystem presented is one that already exists (and is known to the student)	A partial, new cryptosystem is presented but the system is incomplete.	A new cryptosystem is presented that incorporates aspects of established cryptosystems in a new way.	A new cryptosystem is presented that incorporates aspects of established systems along with new, inventive aspects or only contains new, inventive concepts.
The student explained the new cryptosystem including any tools needed.	No explanation of a new cryptosystem is given	The new cryptosystem is partially explained but the explanation is unclear or lacking in details.	The new cryptosystem is fully explained.	The new cryptosystem is fully explained and any special circumstances that may have an impact on the cryptosystem are included in the explanation (for example when numbers are needed).

The student provided examples of encrypting and decrypting using the new cryptosystem.	No examples are provided for encrypting or decrypting using the cryptosystem.	An example of encryption **or** decryption is provided, but not both.	An example of encrypting and an example of decrypting using the new system are provided.	Examples are provided for encrypting and decrypting using the new system as well as any examples that might show special circumstances in which the system might be used (for example, with numbers)
Instruction is created to teach others about the new cryptosystem.	No instruction is created or the instruction created does not make sense.	The instruction created is incomplete or lacking cohesiveness or continuity. The instruction created is confusing.	The instruction created is complete and makes sense. It correctly teaches others how to use the new cryptosystem.	The instruction created is complete and makes sense. It also incorporates inventive strategies for teaching the new cryptosystem.
The student provided at least 3 reasons they believe their system would be secure.	The student provided 0-1 reasons they believe their system would be secure.	The student provided 2 reasons they believe that their cryptosystem would be secure.	The student provided 3 reasons that they believe their cryptosystem would be secure.	The student provided more than 3 reasons that they believe their cryptosystem would be secure.

LESSON #4

The Key to Keeping the Secret

I. DEFINE OBJECTIVES AND CONTENT	
LESSON OBJECTIVE	Students will be able to explain at least one modern use of cryptography. Students will be able to describe at least one way that their new cryptosystem has been improved because of collaboration and **INTERACTIONS** with others.
POINT TO PONDER	Cryptosystems do not always have to be absolutely secure.
ESSENTIAL QUESTION	How has technology played a role in changing cryptography?

CONTENT Outline the content you will teach in this lesson.	10. Cryptography's interaction with Computer Technology A. Creation of secure codes and ciphers allows computer technology to expand and provide more services and information to people B. As computer technology becomes more powerful, cryptosystems used in the past become obsolete C. New cryptosystems and protocols must be created and the field of cryptography grows and expands to address new topics and concepts and the cycle continues 11. Modern Applications A. RSA cipher 1. Created in 1977 by Ronal Rivest, Adi Shamir, and Leonard Adleman 2. Asymmetric cipher where two keys are used--an encryption key and a decryption key 3. Allows people who are unknown to each other to communicate securely 4. Makes use of prime factors of very large numbers so that it takes a lot of time to break the cipher even using the combined power of many computers--this makes it unbreakable in a practical sense B. Data integrity 1. Makes sure that the data being sent has not been changed by a third party while it was in transit 2. Encourages interactions among people because the senders and receivers know that the data has not been changed or tampered with C. Data authentication 1. Determines whether the supposed sender of the data actually sent the data 2. Determines that no one else is pretending to be the person who supposedly sent the message 3. Uses a digital signature that is confirmed by a third party 4. Encourages interactions among people because a receiver has assurances that the alleged sender actually sent the communication

II. PRE-PLANNING

What will students UNDERSTAND as a result of this lesson? How does this connect to the Essential Question?	Students will understand that cryptography has expanded to address issues beyond encryption. Students will understand the difficulties cryptographers face in trying to create a secure cryptosystem. Through these understandings, students will see that the expanding computer technology has caused cryptography to expand and address more issues. The fact that computers make more **INTERACTIONS** possible has caused cryptographers to create systems that make these **INTERACTIONS** more reliable, trustworthy, and secure. The students should be able to use these understandings to explain how computer technology has affected cryptography.
What will students be able to DO as a result of this lesson?	Students will be able to explain at least one issue (other than encryption) that modern cryptography addresses. Students will be able to explain at least one way that their product was improved because of their **INTERACTIONS** with others. Students will be able to use their knowledge of established cryptosystems to create their own cryptosystem. Students will be able to create their own video instruction to teach others their cryptosystem. Students will be able to list at least three reasons that they believe their new cryptosystem is secure.

III. PLANNING	
HOOK Describe how you will grab students' attention at the beginning of the lesson. BE CREATIVE.	TIME: Students will view a video of edited news clips about recent hacking occurrences located at https://drive.google.com/file/d/0B8_Iy2-ce3qlMG9MYzltNTExelU/edit?usp=sharing (2.5 min) After the video, the group will discuss how this relates to cryptography and why cryptography is important. We will make sure to discuss the fact that most of the cryptography used with computers and technology is done without our knowledge and people don't tend to think about it until there is a big breach. However, cryptography makes much of what people do on the internet safe and reliable.
INSTRUCTION Explain Step-by-step what you will do in this lesson. Be explicit about ties to Points to Ponder, Essential Question, and Interactions here. Include ALL support and teaching materials with your unit.	TIME: 60 min. 1. As students enter the classroom, we will return their crypto-journals. 2. After students have viewed the hook video, we will discuss the fact that, although cryptography has been used for millennia, it is still important today. We will briefly review what we learned on Day 3 about how computers have changed the types of encryption needed. We will also mention that computers and technology have caused cryptography to expand to address other issues (essential question). 3. Ask students what they think the other issues addressed by cryptography could be. After listing their ideas, we will tell the students that we will be learning about three modern applications of cryptography. 4. Explain to the students that they will be divided into 3 groups. Each group will be given information about one of the modern applications of cryptography—RSA cipher, data integrity, and data authentication. The students in each group will study the information and determine how they will present the information to the rest of the group so that they can understand it. They could quickly create a skit about it, create a picture about it, create a product using words, etc. (3 minutes to brainstorm and discuss) 5. Students will create whatever they need to present their application and practice their presentation (8 minutes). 6. Students will present their application to the group (3 minute presentation per group). 7. We will make sure to mention that the new RSA cipher is not absolutely secure. If the prime numbers used can be determined, a third party would be able to decipher the

encryption. However, finding these very large prime numbers takes a very long time and a lot of computing power (many computers combined). Therefore, the cipher is secure for all practical purposes. Discuss whether this is as good as using an absolute secure cipher like the one-time pad. Refer to the point to ponder: Cryptosystems do not always have to be absolutely secure.

8. Practice with the theme of **INTERACTIONS**:
   a. Students, in pairs, will be given the pieces to the Changes in Cryptography puzzle (see attached) and will complete the puzzle.
   b. Once they have completed the puzzle, the students will read the information given on the puzzle. (The order of the pieces is indicated by the arrows on the puzzle.)
   c. With their partner, the students will try to figure out a pattern that seems to be occurring in the information provided on the puzzle. (The information on the puzzle contains events from the modern era of cryptography.) The teachers will monitor and rotate around the room to help with this partner discussion. Teachers, if necessary, will help guide students to see that as changes occurred with regards to technology, changes occurred with regards to cryptography and vice versa. Cryptography and computer technology interact with one another.
   d. Students will then return to a whole class discussion and share what they noticed with the information on the puzzle. We will help guide students to predict that this cycle of change will probably continue in the future.
   e. We will refer to the essential question and discuss how expanding technology has changed cryptography.
9. Students will have a Skype conversation with students from D.F. Walker Elementary School. The students at D.F. Walker Elementary School have already participated in this challenge to make a cryptosystem. During this conversation, the students will focus on talking about the positive and negative aspects of the various cryptosystems studied during the week as well as how those positive and negative aspects can be applied to the cryptosystems our students are making and that the D.F. Walker students have already created. During this time the students will also have an opportunity to explain their new cryptosystem or the ideas they have for it briefly in order to receive feedback from any of the students participating. Our camp students should note in their crypto-journals any ideas they think might be helpful in their cryptosystem creation project

(see attachment for guiding questions for this Skype conversation).

10. We will tell the students that by now they should have many ideas about what they want to include in their new cryptosystem. Some pairs have already started creating their system. Tell the students that during the rest of our time and the time this afternoon, they will work on creating the final product we discussed on day 1 and have revisited each day.
11. Remind students that they will be creating video instruction much like the videos they experienced at their stations on Monday and Tuesday. Have students think about what was presented in the video instruction at their stations. (The instruction included a specific example showing how to encipher and decipher using the cipher system. The instruction also showed any tools needed to use the cipher and explained and demonstrated how the tool was used.) Show the group a short video example created by a girl about their age about the Pigpen Cipher located at http://www.youtube.com/watch?v=2XZaffzCuRg. Critique the video with the students. Students should notice that the tool needed to use the Pigpen Cipher is explained and an example is given, but there were some flaws with the recording that made the instruction less effective. For example, the camera angle and distance from the camera made it harder for the learner to understand what was being taught. Therefore, while videoing the instruction for their cryptosystem students should make sure that they are recording at a good angle and a good distance form what they are recording.
12. Teachers will demonstrate how to create a video recording using the iPad by recording a short video using the code book code from earlier in the week. Then as students are planning with their partner, teachers will circulate and open the video recording app on each iPad and provide each group with the written directions of the steps demonstrated by the teachers (see attached).
13. We will review the rubric that was presented yesterday (see attached) so that students know the expectations for the project. We will review with the students how the rubric fits with the cryptosystem creation project form in their crypto-journal (which was also discussed yesterday). We will reinforce (from the rubric) that the instructional video should contain the tools necessary to use their cryptosystem, at least one example using their cryptosystem to encrypt, at least one example using their

cryptosystem to decrypt text (they can include more if they believe it is necessary in order for our "clients" to understand the system), and a statement that contains at least 3 reasons (or aspects of the system) that make the system secure. These reasons or aspects should help the "client" team choose their new cryptosystem as the best one to use for their "Survivor Games" challenge.

14. Students will work with their partner to complete their cryptosystems creation project form (see crypto-journal), create their cryptosystem, plan their instruction, and create their instruction. During this time, students can revisit all of the padlets from the week and their notes in their crypto-journal to help them complete their projects. Teachers will rotate around the classroom and help guide projects as needed.
15. Once students have completed their project, they will create a "worksheet" activity for another group using their new cryptosystem (see attached worksheet form). On this sheet, the students will create a section that requires other students to decrypt text using the new cryptosystem and encrypt text using the new cryptosystem. The example form using the shift cipher (see attached) will be provided for the students to use as a guide. The students may choose to use any format to create the worksheet. If students have a different idea for creating some type of "assessment" about their new cryptosystem, they can present the idea to the instructors for approval.
16. As pairs of groups finish step 15, two cryptosystem creation teams will form a group of 4 students. One team will be the "learning" team while the other team will be the "teaching" team. The "teaching" team will show the "learning" team their instructional video and have the "learning" team complete the worksheet they created to assess their "learning" team's understanding of the "teaching" team's new cryptosystem. The "teaching" team will give the "learning" team feedback about their work on the worksheet and the "learning" team will give the "teaching" team feedback on their instructional video. The "teaching" team will have time once this step 16 is completed to make changes to their instruction to make it more effective, if necessary. Then the "learning" team and the "teaching" team will exchange roles and they will focus on the second group's cryptosystem and video instruction.
17. Cryptosystem creation teams will use the feedback from their partner team to improve their final instructional video.

	18. We will post the final instructional videos on our "secure" website (our Weebly camp session website) so that our clients can view the videos and choose the one that they want to use for their "Survivor Games" challenge. (Our session website will also be open on the iPads during the parent visits so that parents, family, and other students who did not have the opportunity to can view the instruction created by the students during our camp session.) 19. As a group, we will reconvene and discuss the cryptosystems that the class created. Students will have the opportunity to explain their system (briefly) for the benefit of those groups that have not seen it. Then all groups will discuss what they find interesting about their system or other systems created by the group. 20. Students will complete the assessments below. 21. As a final discussion, we will ask the class what they think they will take away from this session this week. Have students share what they might do with their new knowledge in the near or distant future. Also, we will review the theme of **INTERACTIONS**. Students will share the assessment they wrote in their crypto-journal about how their cryptosystem was improved from the **INTERACTIONS** with others. We will remind them that cryptographers typically work with others so that they can make a stronger cryptosystem! Working together this week, we were all more successful!
ASSESSMENT (Performance Task) What will the students DO to demonstrate that they have mastered the content? Be specific and include actual assessment with unit materials.	TIME: 5 min. As their ticket out the door, students will explain on an index card in 1-3 sentences one of the modern applications of cryptography (other than encryption). Students will explain (in their crypto-journal) at least one way that their cryptosystem was improved because of collaboration with others. In this explanation, they will list what the improvement was and what made it an improvement. (How did changing the cryptosystem in that way make the cryptosystem better?) (Connection with the theme of **INTERACTIONS**: Students' **INTERACTIONS** with others have improved their final product.)

DOES THE ASSESSMENT ALLOW YOU TO DETERMINE WHETHER OR NOT THE STUDENTS HAVE MET YOUR STATED LESSON OBJECTIVE? [✓ YES] OR NO

ASSESSMENT AND INSTRUCTIONAL MATERIALS

Insert ALL materials here including Assessments and Instructional Materials.

Explicitly LIST any additional files for this lesson. Be sure that ALL materials have been submitted for this lesson.

Files and links needed for this lesson:
(All of these links are located on our session website. They are also listed in the lesson plan at the appropriate places.)

Hook Video
https://drive.google.com/file/d/0B8_Iy2-ce3qlMG9MYzltNTExelU/edit?usp=sharing

Padlet for Day 1
http://padlet.com/wall/i4r42zpqn8

Padlet for Day 2
http://padlet.com/wall/7ws9ibi3dk

Padlet for Day 3
http://padlet.com/wall/3cq7g0g1od

Example of student created instruction for Pigpen Cipher
http://www.youtube.com/watch?v=2XZaffzCuRg

Attachments for Day 4:

Information sheets for Modern Cryptography Application Activity

RSA cipher

- Created in 1977 by Ronal Rivest, Adi Shamir, and Leonard Adleman

- Asymmetric cipher where two keys are used--an encryption key and a decryption key. The people or systems that encrypt the data do not know the decryption key to decrypt the data.

- Allows people who do not know each other to communicate securely—for example over the internet. This cipher allows business transactions and communication over the internet to happen.

- Makes use of prime factors of very large numbers so that it takes a lot of time to break the cipher even using the combined power of many computers--this makes it unbreakable in a practical sense

Data integrity

- Makes sure that the data being sent has not been changed by a third party while it was in transit

- Encourages interactions among people because the senders and receivers know that the data has not been changed or tampered with

Data authentication

- Determines whether the supposed sender of the data actually sent the data

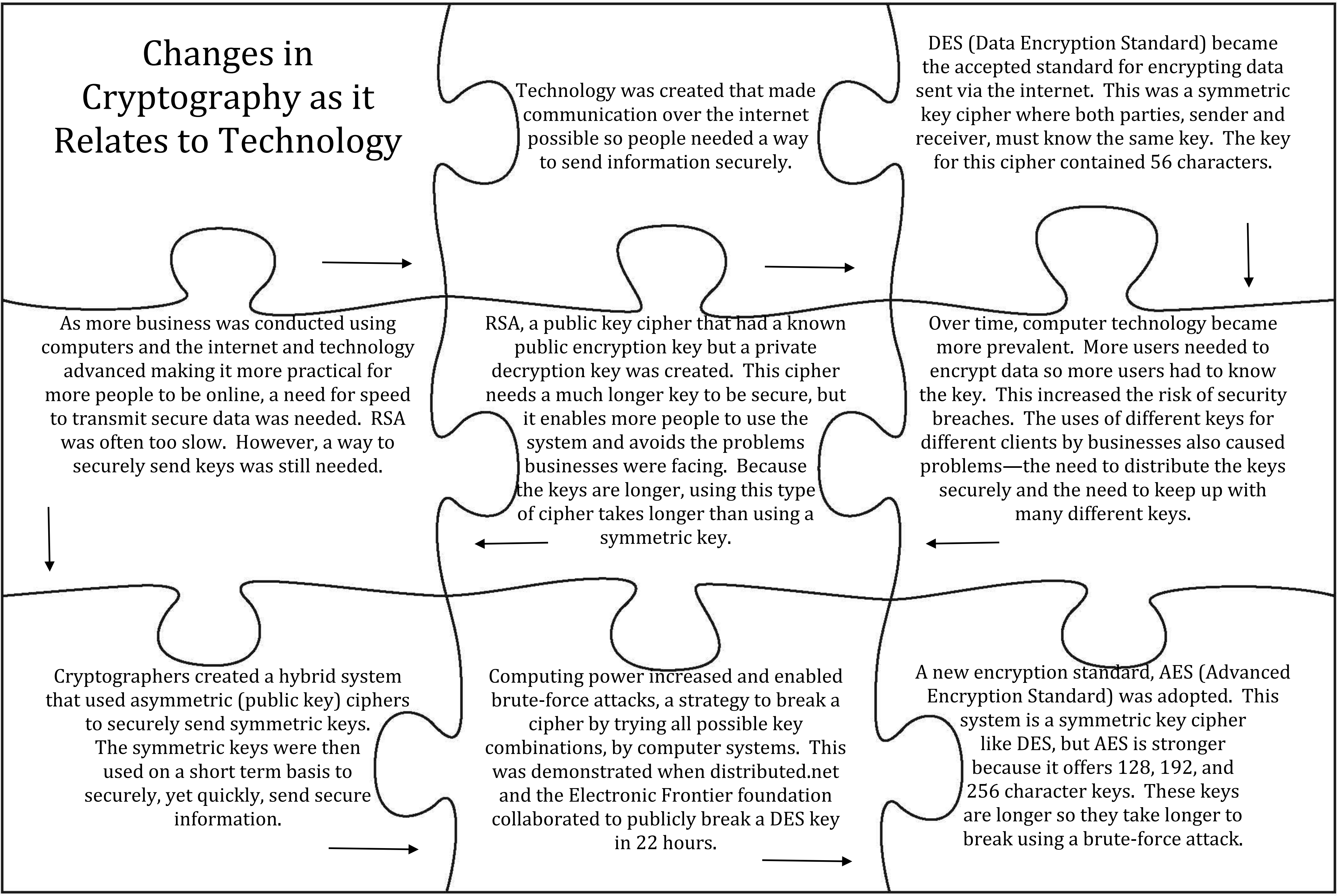
- Determines that no one else is pretending to be the person who supposedly sent the message

- Uses a digital signature that is confirmed by a third party

- Encourages interactions among people because a receiver has assurances that the alleged sender actually sent the communication

Guiding Questions for Skype session
(Students in both groups will be encouraged to freely discuss what they are learning, have learned, are creating, and have created. The following questions will simply guide the discussion so that it remains on topic.)

1. What do you think were the most important aspects of the established cryptosystems you learned about in your stations?
2. Did you think these were positive or negative aspects?
3. Did you make sure to include these aspects in your cryptosystem or did you use the knowledge of them to make your system better in some way?
4. Is your cryptosystem similar to any of the ones we learned about in the stations? How did you make that system better when you created your cryptosystem?
5. What did you notice about creating your cryptosystem that you think could help other students?
6. What were the most important factors you considered in creating your cryptosystem? Did you try to make it really complicated? Did you try to make it simpler so that it could be deciphered or decoded more quickly?
7. What aspect of your cryptosystem do you think is most important in determining that yours is the best and most secure?
8. What can you share with the other students that you think would be most helpful to them in creating their cryptosystem?



Changes in Cryptography as it Relates to Technology

Technology was created that made communication over the internet possible so people needed a way to send information securely.

DES (Data Encryption Standard) became the accepted standard for encrypting data sent via the internet. This was a symmetric key cipher where both parties, sender and receiver, must know the same key. The key for this cipher contained 56 characters.

Over time, computer technology became more prevalent. More users needed to encrypt data so more users had to know the key. This increased the risk of security breaches. The uses of different keys for different clients by businesses also caused problems—the need to distribute the keys securely and the need to keep up with many different keys.

RSA, a public key cipher that had a known public encryption key but a private decryption key was created. This cipher needs a much longer key to be secure, but it enables more people to use the system and avoids the problems businesses were facing. Because the keys are longer, using this type of cipher takes longer than using a symmetric key.

As more business was conducted using computers and the internet and technology advanced making it more practical for more people to be online, a need for speed to transmit secure data was needed. RSA was often too slow. However, a way to securely send keys was still needed.

Cryptographers created a hybrid system that used asymmetric (public key) ciphers to securely send symmetric keys. The symmetric keys were then used on a short term basis to securely, yet quickly, send secure information.

Computing power increased and enabled brute-force attacks, a strategy to break a cipher by trying all possible key combinations, by computer systems. This was demonstrated when distributed.net and the Electronic Frontier foundation collaborated to publicly break a DES key in 22 hours.

A new encryption standard, AES (Advanced Encryption Standard) was adopted. This system is a symmetric key cipher like DES, but AES is stronger because it offers 128, 192, and 256 character keys. These keys are longer so they take longer to break using a brute-force attack.

My Crypto-Journal

Pages from Crypto-Journal to use with Day 4
Including Cryptosystem creation form

Name: ______________________
Session Time: ________________

Day 4

Notes during Modern Cryptography Application activity

Use the space below to write anything that might help with planning and presenting this activity.

Day 4

Notes from Skype conversation

Day 4

Notes to help with Cryptosystem creation

More Notes to help create your cryptosystem

Day 4 assessment:

Explain at least one way that your cryptosystem has been improved through collaboration with others.

Cryptosystem Creation Form

What is the name of your new cryptosystem?

Did you use any aspects of the cryptosystems we learned this week? If so, which one(s)?

List at least 3 aspects of your cryptosystem that you think makes it secure (or at least secure enough for the purposes of this project).

1.

2.

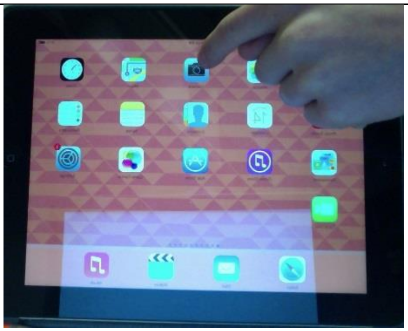
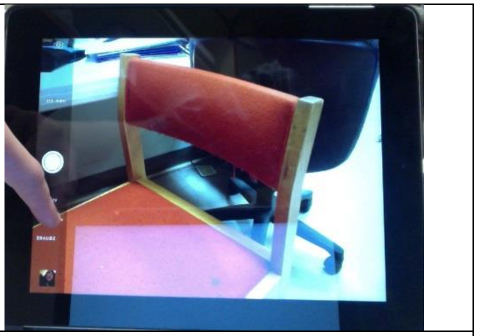
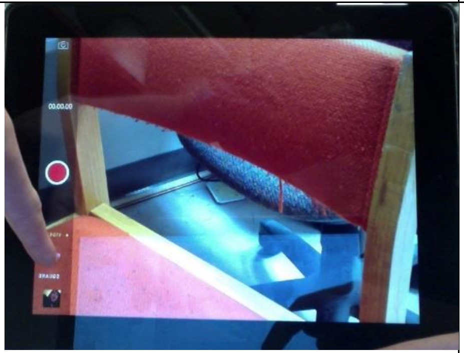
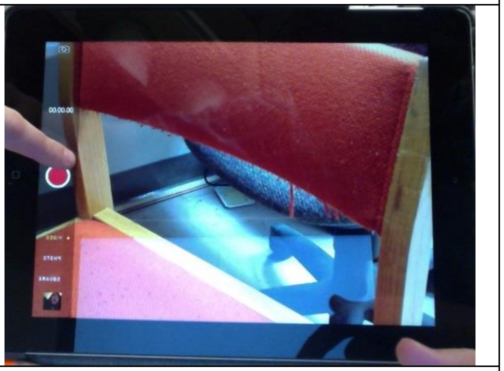
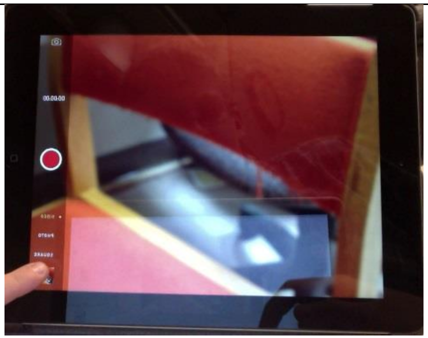
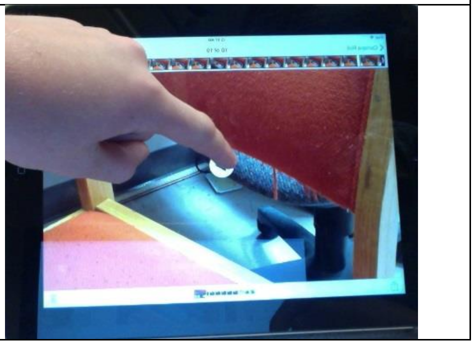
3.

Explain how your cryptosystem works.

Provide at least one example using your cryptosystem.

Plan your video instruction here and on the back of this page.

How to create a video on the iPad

1. Find and click on the camera icon on the iPad – the photo screen should open (make sure your iPad is in landscape when you record.)		**2.** Slide the column that says video, photo and square to video	
3. The white button should turn to a red button. Press the red button to record. (Make sure the camera is on the top left corner of the iPad.)		**4.** The red button should turn into a red square with a white circle around it – you are now recording – press the button again to stop recording.	
5. To view the recording press the square in the bottom right corner.		**6**. Press play to watch the video.	

Directions for creating a worksheet about your new cryptosystem

1. Look at the two example worksheets on the next page to get ideas about how you can set up your worksheet and the type of information you can have your “learner” encrypt and decrypt. The two examples are both on one page, but you will only have one worksheet that you create below. You are not limited to the ideas on these examples. Feel free to use your own ideas, as well.
2. Write the directions for your worksheet. In the directions, tell students what tools (if any) they will use to encrypt and decrypt using your new system.
3. Write information that your “learner” student will need to decrypt using your system. Include any information that the “learner” will need (such as your key).
4. Leave space for your “learner” to write their decrypted answer.
5. Write directions telling the learner the information they should write to encrypt using your system.
6. Leave space for the “learner” to write the plaintext of the information he or she will be encrypting using your system.
7. Leave space for the “learner” to write the encrypted text of the information they wrote in step 5.

New Cryptosystem Worksheet
Cryptosystem Name:_____________________

Decrypting Section:
Directions:

Activity:

Encrypting Section:
Directions:

Activity:

Worksheet examples for Student created worksheet in step 17

Your worksheet could contain a riddle and answer:	*Your worksheet could contain a question about cryptography:*
Decrypting Section: **Directions:** Use your cipher wheel to decipher the answer to the riddle below:	Decrypting Section: **Directions:** Use your cipher wheel to decipher the answer to the question below:
Name four days of the week that start with the letter "t".	How did the Alberti Cipher revolutionize the world of cryptography?
Shift = 8 Bcmalig, Bpczalig, bwlig, ivl bwuwzzwe	Shift = 14 Dzowbhslh zshhsfg ksfs dowfsr kwhv rwttsfsbh qwdvsf hslh zshhsfg wb hvs goas asggous.
Encrypting Section: **Directions**: Use your cipher wheel and a shift of 4 to encipher what you think about our riddle above.	Encrypting Section: **Directions:** Use your cipher wheel to write a question that would have the following answer: The only totally secure cipher
Plaintext thoughts:	Plaintext question:
Enciphered thoughts:	Enciphered question:

Rubric for Index Card Ticket out the Door assessment:

0 pt. Student did not attempt to answer the question
1 pt. Student mentioned an application of cryptography but it was not a modern application
2 pts. Student described an application of cryptography, but it was not a modern application
3 pts. Student wrote the name of a modern application of cryptography, but did not explain it
4 pts. Student wrote 1-3 sentences that fully explained at least one modern application of cryptography

Rubric for Crypto-journal part of the assessment:

0 pt. Student did not list any ways that their cryptosystem was changed because of collaboration with others.
1 pt. Student listed a way that their cryptosystem was changed because of collaboration with others but he/she did not explain how that was an improvement
2 pts. Student listed at least one way that their cryptosystem was changed because of collaboration with others and explained how that was an improvement in the cryptosystem

Rubric for Final Project (All of the following aspects should be evident in the video created.)

	Level 1 Novice 0 pts.	Level 2 Developing 2 pts.	Level 3 Acceptable 4 pts.	Level 4 Outstanding 6 pts.
The student created a new cryptosystem.	No cryptosystem is presented or the cryptosystem presented is one that already exists (and is known to the student)	A partial, new cryptosystem is presented but the system is incomplete.	A new cryptosystem is presented that incorporates aspects of established cryptosystems in a new way.	A new cryptosystem is presented that incorporates aspects of established systems along with new, inventive aspects or only contains new, inventive concepts.
The student explained the new cryptosystem including any tools needed.	No explanation of a new cryptosystem is given	The new cryptosystem is partially explained but the explanation is unclear or lacking in details.	The new cryptosystem is fully explained.	The new cryptosystem is fully explained and any special circumstances that may have an impact on the cryptosystem are included in the explanation (for example when numbers are needed).
The student provided examples of encrypting and decrypting using the new cryptosystem.	No examples are provided for encrypting or decrypting using the cryptosystem.	An example of encryption **or** decryption is provided, but not both.	An example of encrypting and an example of decrypting using the new system are provided.	Examples are provided for encrypting and decrypting using the new system as well as any examples that might show special circumstances in which the system might be used (for example, with numbers)

Instruction is created to teach others about the new cryptosystem.	No instruction is created or the instruction created does not make sense.	The instruction created is incomplete or lacking cohesiveness or continuity. The instruction created is confusing.	The instruction created is complete and makes sense. It correctly teaches others how to use the new cryptosystem.	The instruction created is complete and makes sense. It also incorporates inventive strategies for teaching the new cryptosystem.
The student provided at least 3 reasons they believe their system would be secure.	The student provided 0-1 reasons they believe their system would be secure.	The student provided 2 reasons they believe that their cryptosystem would be secure.	The student provided 3 reasons that they believe their cryptosystem would be secure.	The student provided more than 3 reasons that they believe their cryptosystem would be secure.