Sharon K. Robbert
Trinity Christian College, Palos Heights, Illinois
Sharon.Robbert@trnty.edu

CryptoClue, An Unexpected Topic for a Math Circle

Event #1125-Q5-830, 3:00 Friday, January 6, 2017, Room A701 Atrium Level, Marriott Marquis

Abstract:

Elementary and middle school students may be drawn into interest in mathematics in different ways. Some children enjoy puzzles, games, and secret codes but may not realize how much mathematics is involved in encoding and decoding messages. Cryptography is an excellent tool to support mathematical learning for children at a variety of levels while the children have fun! As one assignment in a course on beginning cryptography for upper-class math and math education majors, college students used cryptography as a basis to design a fun math-based activity for middle school children. The students selected a variety of elementary cryptographic systems to create CryptoClue, a game loosely based on the board game Clue™. At the end of the semester, these same students led approximately 170 middle school math competition participants in playing their invented game. Components of CryptoClue, an overview of the mathematics within the game, extensions for continued mathematical study, simplifications for younger students, resources for learning more about cryptography, and intriguing short and long-term outcomes will be shared.

Three Clues

- The *Where?* clue is hidden on a ribbon by a rearrangement cipher. Cryptosystem: a *scytale*, used in 5th century BC.
- The *Who?* clue is hidden by a shift cipher. Original cryptosystem: Caesar cipher. Tool for deciphering: a Cipher wheel, invented in 15th century AD and used through the American Civil War.
- The *With What?* Clue is hidden by a substitution cipher, where letters are replaced by single-color playing cards. To decipher, earn card-letter assignments by solving practice problems. Substitution ciphers and methods to decrypt were completely understood by Arabs prior to 10th century AD.

Basics of Cryptography

Cryptography is any system of secret writing that allows allies to communicate information accurately with assurance of validity without enemies either intercepting and understanding the message OR tricking allies into believing a false message. Cryptosystems are considered secure if the enemy is unable to decipher the message even if everything about the system is public knowledge except for the key.

Mathematical Extensions

Rearrangement Ciphers:

1. **Geometry:** Encipher a message using the rod of your choice. Then measure the distance between several pairs of consecutive letters in your message. How does this distance compare to the diameter of the rod? How are the diameter and circumference related to the spacing of the enciphered message? What other factors play a role in your cipher? Deliver your enciphered message to another table group to decode.
2. **More Geometry:** If you encipher a single message with rods of differing diameter, one larger and one smaller in diameter, for which rod are the consecutive letters spaced more closely and which farther apart on the ribbon?
3. Alternate Version without Geometry: Rail Fence cipher
   a. Method to encode: write the letters vertically along a set of three (or more) rails, then transcribe horizontally across one rail at a time.
   b. A rail fence message to decipher: **ASOMN MASHE RYGFH EOASK DOORH EIORR**
   c. Online Tool at http://www.simonsingh.net/The_Black_Chamber/railfencecipher.html. Note: remove all spaces between character groups in the online tool.

Shift Ciphers:

1. **Enumeration:** How many different options for a shift cipher exist? How many are valid? Are there any options that are symmetric, that is, plaintext and ciphertext characters are mirrored? E.g., plaintext "a" matched to ciphertext character "#" and plaintext character "#" is matched to ciphertext "A" for ALL letter pairs?
2. **Security:** How secure is this method? How long would it take a determined person to break the cipher?
3. **Modular Arithmetic:** Develop understanding of modular arithmetic. (A =1, B =2, …, Z = 26 = 0 mod 26). What number corresponds to the letter shift in your deciphered clue?
4. More complex ciphering options to consider:
   a. **Vigenère** cipher—use a keyword of an unknown length to determine a cycle of multiple shifts for the plaintext (a Polyalphabetic Substitution Cipher). Note that this method is only a bit more secure than a shift cipher. See http://www.simonsingh.net/The_Black_Chamber/vigenere_cracking.html
   b. **One-time pad**—The keyword in the Vigenère cipher is a random sequence of characters that has the same length as the message. Both sender and recipient have copies of the same keyword pad. Each is used only one time. Note that this is the only known completely secure encryption method...as long as the pair of one-time pads are kept secure.
   c. Suppose you wished to encipher a message with all identical characters, e.g., "F F F F F F F F F … F." Is this possible? How?
5. Another shift cipher message to decipher: **ZYP RZO TYE SCP PHP ACL TDP ESP P**

Substitution Ciphers:

1. **Enumeration:** Random assignment of letters to characters is a second MSC. How many different options exist here?
2. **Security:** Note that this method is only a bit more secure than shift cipher. Letter frequency analysis to identify likely pairing IF the ciphertext is of sufficient length (need more than 100 characters to make this feasible). Think Wheel of Fortune: "RSTNL E". Can also expand decryption analysis to incorporate common digraphs and trigraphs
3. **Uniqueness:** Is it possible to decipher a code to more than one plaintext message? If so, how? If not, why not?
4. More substitution ciphering options to consider
   a. Suppose you are thinking about whether to retain spacing of words in your ciphertext or not. Which makes for a more secure cipher? Why?
   b. Suppose you expand options for plaintext cipher beyond 26 characters in English alphabet. E.g., add punctuation, spaces, numbers, etc. Does this make the system more secure? Why or why not?

Suggested First Cryptography References:

Lewand, R: *Cryptological Mathematics*, MAA 2000. ($39.75 for MAA Members) ISBN: 978-0-88385-719-9

Singh, S: *The Code Book: the Science of Secrecy from Ancinent Egypt to Quantum Cryptography*, Anchor: 1999. ($10.99 on Amazon.com). ISBN: 978-0385495325

Free online cryptography tool: http://www.simonsingh.net/The_Black_Chamber/chamberguide.html

Beissinger, J. & V. Pless: *The Cryptoclub. Using Mathematics to Make and Break Secret Codes*. AK Peters: 2006. ($41.77 on Amazon.com). ISBN: 978-1568812236

Fiction/Films that utilize cryptography as a plot element:

- Sir Arthur Conan Doyle, "The Adventure of the Dancing Men"
- Eoin Colfer, *Artemis Fowl* series, 8 books (2001-2012)
- Cory Doctorow, *Little Brother* (2008)
- Neal Stephenson, *Cryptonomicon* (some mature content, 1999)
- BBC TV show: *The Bletchley Circle*. (Two seasons, 2012-2014)
- Film: *The Imitation Game* (PG-13, 2014)
- Film: *Sneakers* (PG-13, 1992)