CryptoClue

An Unexpected Topic for a Math Circle

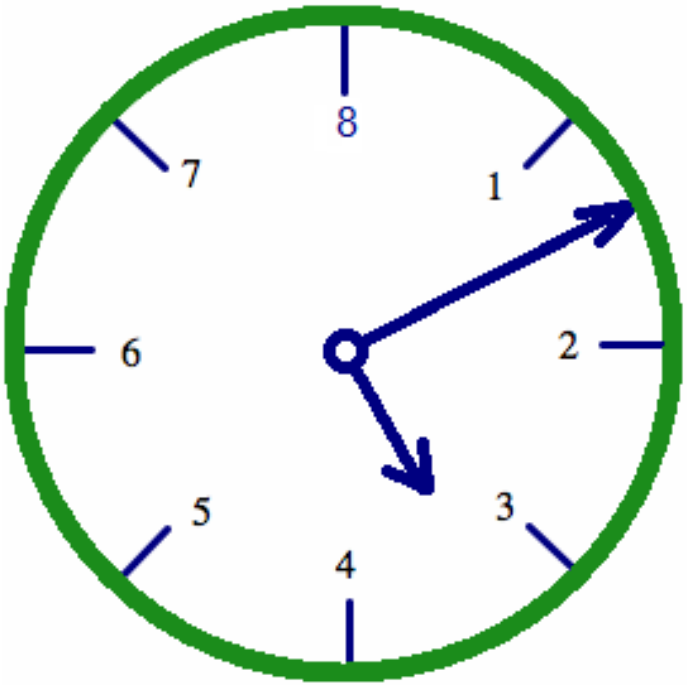
Sharon K. Robbert

Trinity Christian College

January 6, 2017

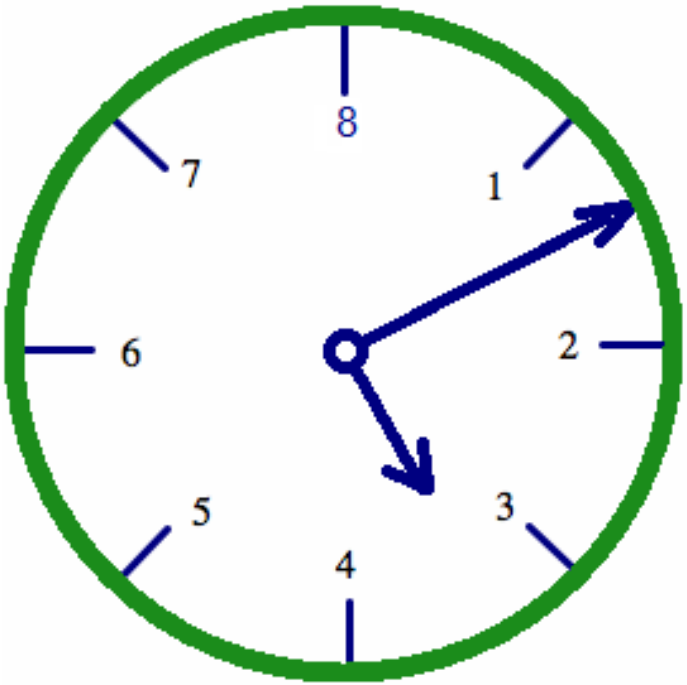
An Hour-able Crime!

- Location: Archimedes Junior High



An Hour-able Crime!

- Location: Archimedes Junior High



- Principal: **Mrs. Bletchley**
- To solve this **enigmatic** mystery, you will need to solve three clues based on historical cryptosystems.
  - Where?
  - Who?
  - With what?

Narrowing the Options

- Principal Bletchley has identified the following options for the crime:
  - Locations for the criminal act: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet
  - Many weapon options, including: a dustbuster, a tennis shoe, a plunger, a squirt gun, shrubbery, bagpipes, etc.
  - Her list of usual suspects:

Narrowing the Options

- Principal Bletchley has identified the following options for the crime:
  - Locations for the criminal act: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet
  - Many weapon options, including: a dustbuster, a tennis shoe, a plunger, a squirt gun, shrubbery, bagpipes, etc.
  - Her list of usual suspects:

- Volunteer crytanalysts?

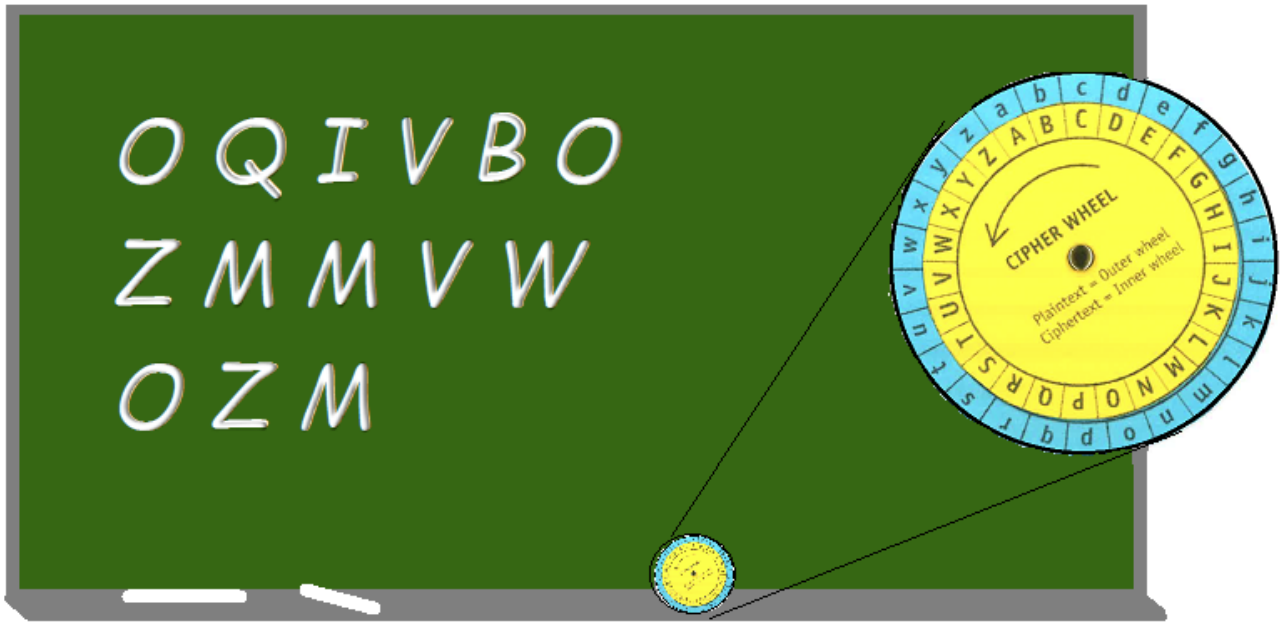
Where? Clue #1: Letters Inscribed on Colored Ribbons

- Curious rods in **Mrs. Oiler's** geometry classroom, ribbons dangling from light fixtures

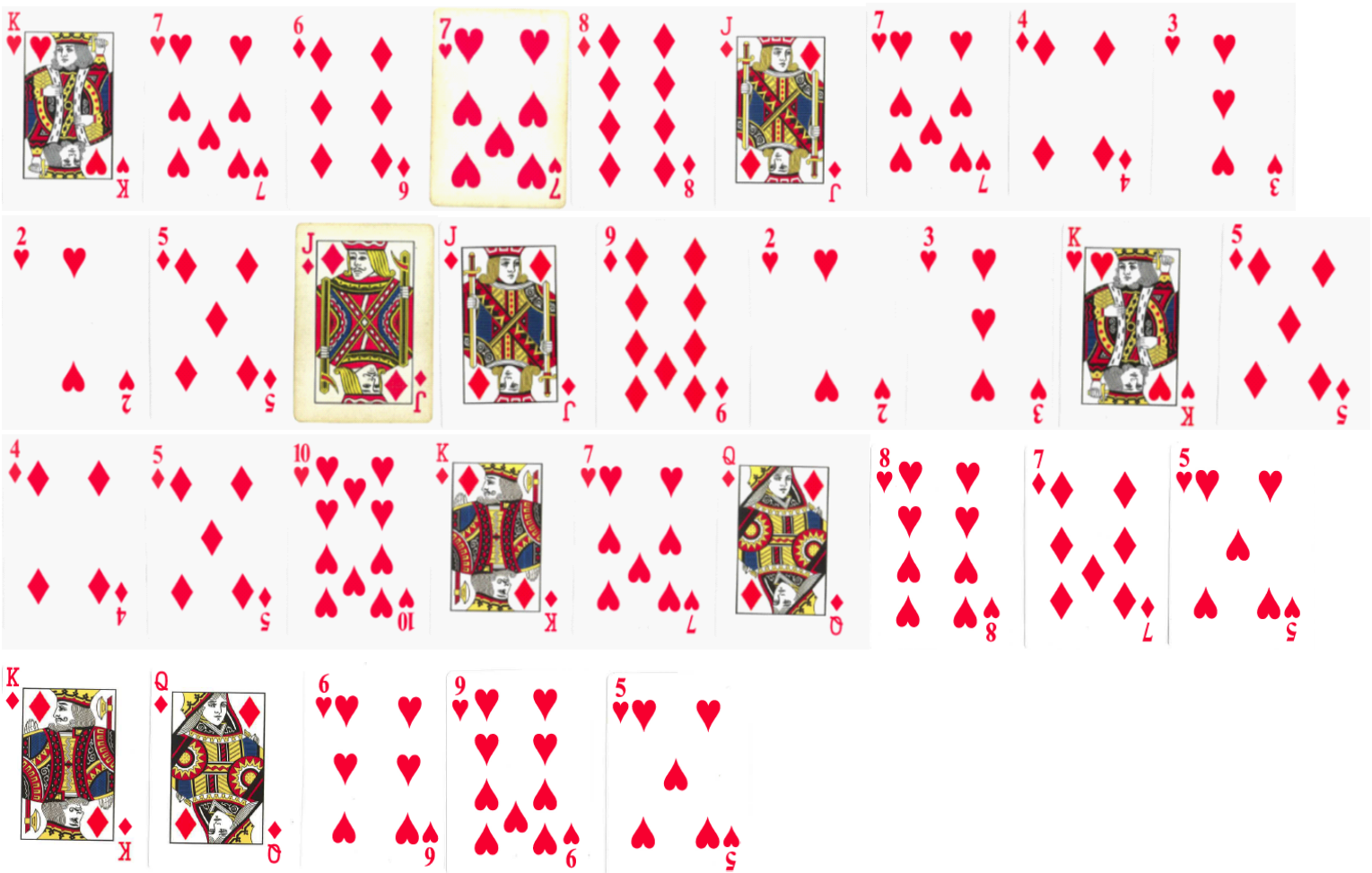
- Hint: To solve the riddle, you must test the ribbons by wrapping them around the rods provided to see if the resequencing makes sense.

Who? Clue #2: A Cipher Wheel and Cipher Text

- In **Mr. Seezer's** classroom:



With What? Clue #3: A sequence of playing card symbols of one color



With What? Clue #3: A sequence of playing card symbols of one color

- Curious fact: the number of red playing cards is identical to the number of letters in the English alphabet.
- A suspicious challenge by your math tutor, **Ms. R.S. Adleman:** "I'll give you one card-letter clue for each correct problem you answer..."
- Hint: you need not obtain all 26 cards to solve the riddle and determine the weapon of clock destruction.

What is Cryptography?

- Any system of secret writing where
  - allies can communicate information accurately
  - allies are able to be assured of information validity

What is Cryptography?

- Any system of secret writing where
  - allies can communicate information accurately
  - allies are able to be assured of information validity
- BUT where
  - enemies cannot understand an intercepted message
  - enemies cannot trick allies into believing a false message

What is Cryptography?

- Any system of secret writing where
  - allies can communicate information accurately
  - allies are able to be assured of information validity
- BUT where
  - enemies cannot understand an intercepted message
  - enemies cannot trick 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. (Kerckhoffs' principle)

Historical Notes

- Where? Clue #1: Letters Inscribed on Colored Ribbons
  - The ribbons and tubes are a modern version of an ancient Spartan cipher tool called a **scytale** from the fifth century BC

Historical Notes

- Where? Clue #1: Letters Inscribed on Colored Ribbons
  - The ribbons and tubes are a modern version of an ancient Spartan cipher tool called a **scytale** from the fifth century BC
- Who? Clue #2: A Cipher Wheel and Cipher Text
  - The cipher used in this clue is a shift cipher, a variation of the Caesar cipher.

Historical Notes

- Where? Clue #1: Letters Inscribed on Colored Ribbons
  - The ribbons and tubes are a modern version of an ancient Spartan cipher tool called a **scytale** from the fifth century BC
- Who? Clue #2: A Cipher Wheel and Cipher Text
  - The cipher used in this clue is a shift cipher, a variation of the Caesar cipher.
- With What? Clue #3: A sequence of playing card symbols of one color
  - The cipher used in this clue is a substitution cipher, believed to be first used by Arabs prior to the 10^{th} century AD. The Arabs also were the first to do frequency analysis of characters to break these codes!

Crime Resolved!

- Where: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet

Crime Resolved!

- Where: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet
  - Clue: *Sometimes this possibly scary and dark place is called the cellar or the lower level but most people just call it this eight letters.*

Crime Resolved!

- Where: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet
  - Clue: *Sometimes this possibly scary and dark place is called the cellar or the lower level but most people just call it this eight letters.*
- Who:

Crime Resolved!

- Where: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet
  - Clue: *Sometimes this possibly scary and dark place is called the cellar or the lower level but most people just call it this eight letters.*
- Who:
  - Clue: *Giant Green Ogre.*

Crime Resolved!

- Where: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet
  - Clue: *Sometimes this possibly scary and dark place is called the cellar or the lower level but most people just call it this eight letters.*
- Who:
  - Clue: *Giant Green Ogre.*
- With What: a dustbuster, a tennis shoe, a plunger, a squirt gun, shrubbery, bagpipes, etc..

Crime Resolved!

- Where: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet
  - Clue: *Sometimes this possibly scary and dark place is called the cellar or the lower level but most people just call it this eight letters.*
- Who:
  - Clue: *Giant Green Ogre.*
- With What: a dustbuster, a tennis shoe, a plunger, a squirt gun, shrubbery, bagpipes, etc..
  - Clue: *I am a plant collection of hardy shrubs.*

Crime Resolved!

- Where: Outhouse, Walk-in closet, basement, Tree house, Attic, kitchen cabinet
  - Clue: *Sometimes this possibly scary and dark place is called the cellar or the lower level but most people just call it this eight letters.*
- Who:
  - Clue: *Giant Green Ogre.*
- With What: a dustbuster, a tennis shoe, a plunger, a squirt gun, shrubbery, bagpipes, etc..
  - Clue: *I am a plant collection of hardy shrubs.*
- **The clock crime was committed by Shrek with shrubbery in the basement.**

Overview of CryptoClue Development

- Crypto Puzzles were created by a cryptography class of 13 college students several years ago

Overview of CryptoClue Development

- Crypto Puzzles were created by a cryptography class of 13 college students several years ago
  - One is completing a Ph.D. in philosophy

Overview of CryptoClue Development

- Crypto Puzzles were created by a cryptography class of 13 college students several years ago
  - One is completing a Ph.D. in philosophy
  - Four are working in computing fields
    - Brandon: "...cryptography showed the mysterious side of mathematics, and that sometimes math can be used for fun instead of 'solving problems'..."
    - Maria: "...the familiarity with cryptography and the history and purpose behind it has definitely boosted my ability to contribute to [a] work project" implementing a data obscuring tool

Overview of CryptoClue Development

- Crypto Puzzles were created by a cryptography class of 13 college students several years ago
  - One is completing a Ph.D. in philosophy
  - Four are working in computing fields
    - Brandon: "...cryptography showed the mysterious side of mathematics, and that sometimes math can be used for fun instead of 'solving problems'..."
    - Maria: "...the familiarity with cryptography and the history and purpose behind it has definitely boosted my ability to contribute to [a] work project" implementing a data obscuring tool
  - Eight are teaching mathematics,
    - Lauren: I created "a cryptography lesson in Algebra 2 as a tie to inverse functions."
    - Dan: Cryptography "tied together history, humanities, technology, and of course mathematics in a way that made me feel like I was learning 'just for the fun of it.'"

Trinity Math Triathlon Half-time

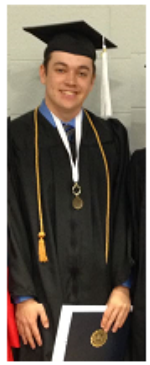
- CryptoClue was played with approximately 170 junior high students in a 45 minute window with 24 different sets of clues

Trinity Math Triathlon Half-time

- CryptoClue was played with approximately 170 junior high students in a 45 minute window with 24 different sets of clues
- Student response
  - The shift cipher was very challenging for the students, even with cipher wheel provided.
  - The students very quickly solved the scytale puzzle.

Trinity Math Triathlon Half-time

- CryptoClue was played with approximately 170 junior high students in a 45 minute window with 24 different sets of clues
- Student response
  - The shift cipher was very challenging for the students, even with cipher wheel provided.
  - The students very quickly solved the scytale puzzle.
  - Spencer: After the Triathlon, "I ended up buying a book with a bunch of cryptography-related puzzles" to solve the following summer...



Math Circle Event

- Challenge teachers to solve the puzzles with guided instruction in each cryptosystem

Math Circle Event

- Challenge teachers to solve the puzzles with guided instruction in each cryptosystem
- Why cryptography as a topic?

Math Circle Event

- Challenge teachers to solve the puzzles with guided instruction in each cryptosystem
- Why cryptography as a topic?
  - Many applications to middle school and high school mathematics curriculum!
    - Math topics in cryptography include: geometric measurement, function characteristics, modular arithmetic, statistics (frequency analysis), number theory
    - More ideas (and puzzles to try!) on handout

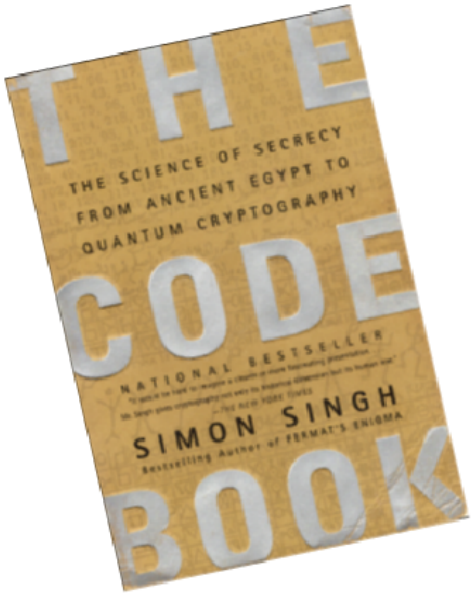
Math Circle Event

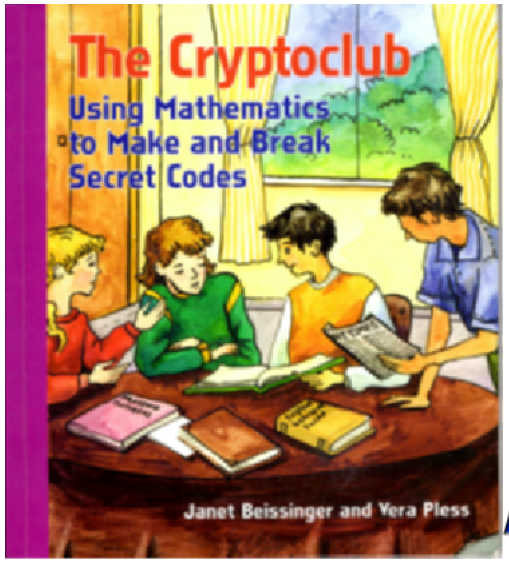
- Challenge teachers to solve the puzzles with guided instruction in each cryptosystem
- Why cryptography as a topic?
  - Many applications to middle school and high school mathematics curriculum!
    - Math topics in cryptography include: geometric measurement, function characteristics, modular arithmetic, statistics (frequency analysis), number theory
    - More ideas (and puzzles to try!) on handout
  - Great way to link to other subjects!
    - Historical context of cryptography: story characters, use of cryptography in intrigue and war
    - Literature involving cryptography as plot element
    - Current technology: secure online transactions, passcodes for devices, E-currency

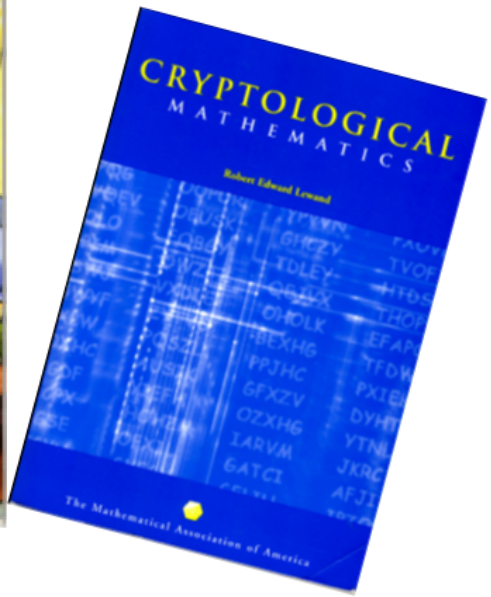
Math Circle Event

- Challenge teachers to solve the puzzles with guided instruction in each cryptosystem
- Why cryptography as a topic?
  - Many applications to middle school and high school mathematics curriculum!
    - Math topics in cryptography include: geometric measurement, function characteristics, modular arithmetic, statistics (frequency analysis), number theory
    - More ideas (and puzzles to try!) on handout
  - Great way to link to other subjects!
    - Historical context of cryptography: story characters, use of cryptography in intrigue and war
    - Literature involving cryptography as plot element
    - Current technology: secure online transactions, passcodes for devices, E-currency
  - It's FUN and can be used to excite students about mathematics

Recommended Beginning Cryptography References







- Online cryptography tool: http://simonsingh.net/The_Black_Chamber/

Fiction and Films that Utilize Cryptography as a Plot Element

- Sir Arthur Conan Doyle, *The Return of Sherlock Homes* "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" (2014)
- Film: "Sneakers" (1992)

Conclusion

Questions?

Contact Information:

Sharon Robbert
Trinity Christian College
sharon.robbert@trnty.edu

Special thanks to Trinity's maintenance department for cutting the twenty-four sets of scytales!

Extensions: Rearrangement Ciphers

- Scytale uses a geometric pattern to rearrange letters. Extension questions:
  - Encipher a message using the rod of your choice. Then measure the distance between several pairs of consecutive letters. How does this distance compare to the diameter of the rod?
  - 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?
  - Give your encoded message to another table group to decipher.
- Another similar cipher to investigate: rail fence cipher

Extensions: Shift Ciphers

- How secure is this method? How long would it take a determined person to break the cipher?
- How many different options for shift cipher exist?
- Are there any shift ciphers that are symmetric, that is, where plaintext and ciphertext are mirrored?
- Shift ciphers can be interpreted in terms of modular arithmetic with mod 26. What number corresponds to the letter shift used to decipher your clue? What number corresponds to the letter shift used to encipher your clue? What is special about these number pairs?
- More complex versions of shift ciphers
  - Vigenere cipher: use a pattern of multiple shifts in a single message, usually based on a keyword.
  - One-time pad: each letter in the message is shifted by a random letter sequence recorded on the pad.
  - Suppose you wished to encipher a message with all identical characters, e.g., "F F F F F F F F F F... F." Is this possible? How?

Extensions: Substitution Ciphers

- How many different options for encoding a 26 character message with a substitution cipher exist?
- Cipher security is not solely based on the number of options: letter frequency analysis for ciphertext of sufficient length
- Common English digraphs (th, er, on, an, re, ...) and trigraphs (the, and, tha, ent, ion, ...) can also be used to complete the cryptanalysis.
- Is it possible to decipher a code to more than one plaintext message? If so, how? If not, why not?
- Other versions of substitution ciphers
  - Retain word spacing vs. uniform letter blocks. Which makes for a more secure cipher? Why?
  - Expand character set beyond the 26 letters. E.g., add punctuation, numbers, spaces, etc. Does this make the system more secure? Why or why not?