Cryptography: Decoding a Murder

Lesson Type: Module
Target Grade: Elementary
Author: Ashley Chen & Tiffany Ma
(Morse Code module modified from Akshay Belur & Melissa Joseph's Spring 2015 lesson on Telegraphs)
Semester: Fall 2016

Brief Overview

Our lesson revolves around a murder mystery that the students have to solve through deciphering. In the last optional part of the lesson, students will utilize what they've learned to make their own own ciphers/codes.

Teaching Goals

- Teach the logic of encoding information through binary systems (through yes/no questions)
- Understand the main components of a cipher (plaintext, ciphertext, and key) and the differences between the two types of classical ciphers (substitution and transposition)
- Allow students to explore different ways to encode information

Agenda

- Intro/Module 0: Intro activity of each student asking yes/no questions to learn (5-10 mins)
    - That a named mentor has been murdered
    - An unnamed mentor is the murderer
- Module 1: Use Morse Code to learn how the victim died (15-20 mins)
    - Spoiler alert: "pushed off a cliff"
- Module 2: Deciphering two separate pieces of information (15-20 mins)
    - Which when put together, tells you who the murderer is
- Module 3: Making your own cipher/code (optional, time permitting)
    - To store your own secret

Module 0: Lesson Introduction - Yes/No Questions

Introduction

- This activity introduces the basic concept that any piece of information can be obtained by asking a series of yes/no questions.
- This is in fact how, on a low-level, classical computers work. A voltage drop across a logic gate encodes a '1', whereas no voltage drop encodes a '0'. More complicated information can be built from these building blocks.

Background/Notes for Mentors

- This lesson gets into the idea of how one encodes information. In the module, we are encoding information using a 'yes' or a 'no', much like a computer encodes information using a '1' or a '0'.
- It is a mathematical fact that, no matter how complicated the information you are trying to encode, it can always be done in a way where you reduce it down to '1's and '0's.
- Information is measured in 'bits', which is a shorthand for **bi**nary digi**ts**.
- This lesson focuses on classical logic, which is the basis of how all current computers work.
- A new research field is slowly emerging, however, called quantum logic, in which the manner of encoding information is more complex, but allows you to encode more information using the same amount of 'space'.

Concepts to Teach

- We will teach the kids that you can get a lot of information from just asking yes/no questions - and that this is how computers work at the most basic level!

Materials

- A bean-bag to pass around the circle

Procedure

- Students should be gather into a circle
- Once gathered, one mentor will explain that **a crime has happened, and it involves people in this room.** The students are the detectives, and **in order to get more information about the crime, they can only ask Yes/No questions**.
- Pass the bean bag around the circle: the student holding it will ask a Y/N question
  At the end of the game, they will obtain the information that
  - there has been a **murder**
  - the **identity of the victim (named mentor** e.g. Bernardo**)**
  - Murderer is an **UNNAMED** mentor (e.g. Caroline but they cannot know!)
- We will proceed counterclockwise, going forward until the kids converge on the information.

IMPORTANT! If they start guessing who the murderer is, stop and say that you are not allowed to answer.

Module 1: Morse Code - figure out the *Cause of Death*

Introduction

- This module will introduce to students a simple method of sending and receiving a coded message - the Morse Code.
- Students will work in groups to learn how the victim died - namely, they have been **pushed off a cliff**. □

Background about Morse Code

- Telegraphs were invented in the 1800s. They work by sending electrical signals (short bursts of current) along wires.
    - Short bursts = "." and long bursts are the "-"
- Samuel Morse pioneered the use of the telegraph, creating his own code made of long and short beeps corresponding to different letters of the alphabet.
- Before, ships carried messages that took weeks to arrive. A telegraph line across the bottom of the Atlantic Ocean in the mid-1800s made communication super fast!
- (The name Morse code is misleading because it is a cipher, NOT a code! *gasp*)

Procedure

- Ask students, "before the internet and before phones, how did people communicate quickly with each other?
    - Briefly go over some of the history of a telegraph described above (maybe not all of it since it is a little boring but whatever you see fit).
- Students should get into pairs (or groups of three, depending on size of site and number of buzzers) and sit back to back
- Mentors will give first student in each pair the circuit and the coded message
    - Let them build the circuit if you see fit with time & their abilities. We will provide a printed diagram of the circuit that they can follow to build it, so it should not take too long. This can become a part of the competition to see which group figures out the message first. This is also a fun and more interactive/hands-on component that would be good to include if you think your site's students will be restless from the paper-based deciphering activities.
- The other student will receive a pencil and the printed key
- The student with the circuit will send the message, and the student with the key will figure out the message being sent to them
- Note: Keep an eye out for students that might try to "cheat" by simply sharing the coded message and key with each other rather than transmitting the message and decoding it!
- They should figure out the cause of death: **"PUSHED OFF A CLIFF"**

Material to Teach

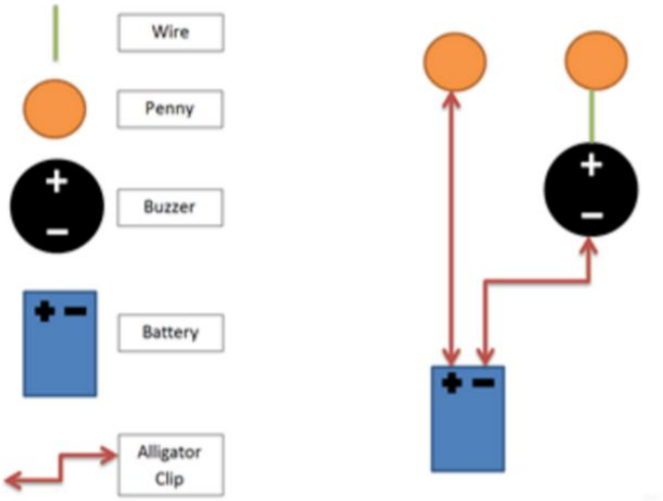
- Continuing from module 0, more complex information can be built up from simple 2-state systems
    - Different combinations of long beeps and short beeps to get different letters of the alphabet
- The focus of this lesson is not on circuits/electricity, so we will just tell the students that touching the pennies together will cause the buzzer to beep. The longer they hold the pennies together, the longer beep they will get!

Materials

- Copper wire
- Buzzers
- Batteries
- Pennies
- Tape
- Alligator Clips
- Pencils
- Sheets with the Morse code key
- Sheets with the coded message “pushed off a cliff” in Morse code

Background/Notes for Mentors on Procedure

- We will set up the circuits for the students ahead of time, if you think that the students are going to have a lot of trouble building it!



    - Alligator clips connect directly to the battery terminals
    - Use tape to attach wire firmly to one side of the two pennies
    - Tape can’t cover the contacts or the switch will not work
    - To attach wire to buzzer, stick through the little hole and bend the wire to connect it securely
    - Use tape loops to attach the pennies to the cardstock paddles, one on top, one on the bottom, with the non-wired side
    - Make sure the polarity is correct (negative end of the battery connected to the negative end of the buzzer)

Module 2: Deciphering Activity

WHAT MENTORS HAVE TO WEAR

Half of mentors: Wear anything that's blue WITHOUT the word "Berkeley"
Other half of mentors: Wear Berkeley WITHOUT Blue
Murderer (most important): Wear BLUE SHIRT/ SWEATER that says "BERKELEY"

THE CLUES THAT STUDENTS RECEIVE

Half the class gets the clue: WEARINGABLUESHIRT
Other half gets: BERKELEYSHIRT

Introduction

- This section will be to show the students how decryption works. Furthermore, they should be able to realize that without the decoding algorithm, the letters would make no sense.
- In relation to ___'s death, we will say that two witnesses saw parts of what happened during the murder, but that they want to send coded messages so that the messages don't get in the wrong hands.
- By the end of this module, all students should have figured out who the murderer was

Materials

- Paper for the code to give to the students, and scratch paper for the students to use to decipher the code.

Background/Notes for Mentors

- A cipher is an **algorithm** - mechanical/mathematical operations that can be performed step by step.
    - For example, one cipher algorithm could be: replace each letter with the number given by (n+5), where n is the numbered position that a letter holds in the alphabet (e.g. A=1, B=2, C=3)
        - Thus, the word "cap" enciphers to the number 8619
- This is different from a code - a code maps a meaningful unit (e.g. a word or phrase) into a different meaningful unit (e.g. a different word or phrase)
    - The important difference here is you can't work a mathematical operation backwards to get the original message. You have to have a list of all the mappings, known as a codebook, or else the coded message makes no sense
    - For example, you could encode the entire sentence "I want to be a scientist when I grow up" to a single word like "Hello!" or to a shorter phrase like "I like cats"
- The main components of a cipher are: plaintext, ciphertext, key
    - Plaintext = the original/deciphered message
        - The plaintext in the above cipher example is "cap"
    - Ciphertext = the encrypted message
        - The ciphertext in the above cipher example is "8619"

    - Key = a piece of information that determines how the cipher algorithm is operated. Also necessary to perform decryption.
        - The key in the above cipher example is the number 5. If the key is changed to a different number, like 7, the algorithm is changed
- Classical ciphers, the type that we will be dealing with, can be split into two categories.
    - One type is the **substitution cipher**, which involves replacing each letter with a new one/ a different symbol. Units of plaintext are **replaced** by units of ciphertext.
        - For example, you could replace each letter with the one after it alphabetically to encrypt, and then rotate back by one to decrypt.
        - The substitution cipher we will use in this module is ROT-13, in which each letter is replaced by the one 13 further along in the alphabet. ROT-13 is special because the encoding and decoding algorithms are identical.
    - The other type is the **transposition cipher**, where the letters are **rearranged** in a new order. The units of plaintext remain **unchanged**, they are simply rearranged.
        - The transposition cipher we will use in this module is the Rail Fence Cipher. The letters are written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached. When the top rail is reached, the letters are written downwards again until the entire message is written out.
- In general, to decrypt such ciphers, all one needs to do is know the algorithm and work backwards.
- Comparison of codes and ciphers *(don't need to teach)*
        - Codes are simpler because no calculations are required. One only needs to lookup parts of the message in the codebook. They are a great way for transmitting information a lot faster because a very long phrase or sentence can be simplified to a single word or much shorter phrase.
        - Because there isn't a fixed system/algorithm for associating plaintext units with ciphertext units, a code can fail gracefully. I.e. An enemy can figure out a few phrases, but still be completely unable to interpret others
        - Codes can only send messages that can be expressed in terms that are in the codebook, but ciphers can transmit all possible messages
- Background on cryptography and connection to cyber security *(don't need to teach)*
    - Cryptography allows for the secure transfer of data and protection of files
    - Important since the Internet is very public but we now use it to store and transfer a lot of private information, such as credit card numbers when making purchases, medical records, etc.
    - Important for the military, national intelligence as well
    - Encryption software uses an encryption scheme so that it can't be recovered without the correct key
    - The ciphers we use in this lesson are from classical cryptography and modern ciphers are much more complicated. They're very different in fact and too complicated to go into, but classical cryptography is still useful for understanding

the basic ideas behind how we can hide messages for protection

Material to Teach & Activity to Demonstrate

- For middle schools (or if you think your site won't get confused by the extra terminology), teach the difference between a code and a cipher. Otherwise, this is background information for mentors to know in case a student asks/is curious.
- Introduce the 3 main components of a cipher
- Explain the two types of classical ciphers. To help demonstrate the difference between the two, ask volunteers to come up for a brief activity:
    - Substitution cipher - A substitution cipher involves **replacing units** of plaintext with new units. Thus, we can replace a letter in the alphabet with a human pose/dance move/facial expression!
        - We will encipher the message "I love BEAM" by having 9 students come up to the front of the class, line up in a horizontal row, and hold a pose of their choice
        - There are two letter E's, so the two students that represent those will have to make the same pose. All the other volunteers should have a different pose.
        - The plaintext units are the English alphabet letters. The ciphertext units are the students' poses.
    - Transposition cipher - Keep the same volunteers and tell them to keep their poses, but ask them to **rearrange** themselves into 2 rows like this: (this is the rail fence cipher that they will use later)

I O E E M

L V B A

Procedure

- For MIDDLE SCHOOLS (or if you think appropriate): To bridge between Module 1 and 2, start by telling the mentees that the name Morse Code is actually misleading, and it's a cipher, not a code! Ask if anyone knows what the difference is before explaining.
- For ELEMENTARY SCHOOLS: Bridge between Module 1 and 2 by saying that Morse Code is just one way of encrypting information. Now we will explore other ways!
- Teach the students about the two ciphers as a whole class, including the interactive encipherment of the phrase "I love BEAM" to demonstrate the difference between the two.
- Ask the volunteers from the activity to sit down, and split the class back into the groups they were in for Module 1. Each group will get both the transposition cipher and the substitution cipher and will have to work to decode them together.
- Pass out the paper with both cipher texts and the ROT-13 wheel to each group, as well as scratch paper and writing utensils. Don't tell them they keys yet though, or which

message is which type of cipher! Let the students try to start decoding the messages.
    - The point of this is that they will notice it is necessary to have a key for decryption to be possible!
    - Let them work on it for about a minute before telling them the keys (or less than a minute, up to your discretion, if they seem too frustrated/ are no having fun)
- The first message will be "wibsternalehragui", which decodes to "wearingabluesweatshirt" using the transposition cipher. We will tell them that there are 3 rails. When they write it out, they should get this:

  w……i……...b…….s……t
  …...e……...r……n……a……..l……e……h……..….r……
  …….a…….g……u……..…i…….

- The second message will be "orexryrlfuveg", which decodes into "berkeleyshirt" using rot-13. We will give them rot-13 wheels to use to help them decode the message.
- Each group should work on only one message at a time. They can choose to start with either one before moving to the second one.
- We will make it a competition to see which group finishes fastest and reward the teams for finishing with candy. When a group finishes, they should tell the mentors who they think is the murderer secretly, so they don't reveal to all other groups who the murderer is
- If there is time remaining, direct the groups that have finished to write their own code (module 3)

Module 3: Writing your Own Code (Optional, if time permits)

Introduction

- In this module, students will use what they've learned to create their own ciphers/codes and send each other messages.

Materials

- Paper
- Pencils or markers

Background/Notes for Mentors

- They can encode whatever they want, or to keep with the theme of the lesson, we can ask them to say which mentor they were most suspicious of at the beginning/looks most like a murderer
    - Emphasize that if they do this, they must use a **mentor's** name (we don't want them being mean to each other)

Material to Teach

- Explain the basic mechanism of information encoding and decipher, encourage the mentees to use the rules and examples leaned in class to create their own code to communicate with another group. Whoever uses the most logical but complicated codes win!

Procedure

- The students no longer have to work in groups, they can make their own ciphers/codes!
- Pass out paper and writing utensils
- If a mentee can't think of how to make their own cipher, some options are:
    - Use the ciphers we covered in Module 2 (ROT-13 or rail fence), but encipher your own message for someone else to decipher
    - Replace a letter with a number
    - Replace a letter with a symbol/drawing (such as a triangle or a heart)
    - Use the ROT-13 wheel, but change the key 13 to a different number
- When finished, they can exchange their messages and keys/codebooks with each other or with mentors to decipher

Summary Materials Table

Material	Amount per Group	Expected $$	Vendor (or online link)
1 bean bag	For the whole site		
Paper with Morse code key	1 (per group)		
1 paper with printed Module 1 ciphertext	1 (per group)		
Printed ROT-13 wheel	1 (per group)		
1 paper with Module 2 ciphertexts printed on them	1 (per group)		
Paper			

pencils/markers			
Candy			
Battery	1 (per group)		
wires	4 (per group)		
Alligator clips	2 (per group)		
Pennies	2 (per group)		