Elcome-way otay EAMBay!

Evan Chin, David Paner | Spring 2021
Adapted from: bumblebeams, Fall 2020
(Priyanka Kannabran, Nicole Chiang, Joelle Chuang, & Austin Nguyen)

Field(s) of Interest: Cryptography

Brief Overview (1-3 sentences):
Written and spoken communication are fundamental parts of our daily lives. Every day, we give and receive information through verbal and transcribed messages. Sometimes, however, we wish to add some secrecy and security to our messages, so that only certain people can understand the true meaning of our messages, and we can keep eavesdroppers out of the loop. This is where cryptography comes into play, allowing us to code our messages using patterns that can only be understood by those who know the secret behind the patterns.

Agenda:
- Module 0: Welcome to BEAM! (10-15 min)
- Module 1: Secret Messages (15-20 min)
- Module 2: Ciphers (15-20 min)
- Conclusion (5 min)

Main Teaching Goals/Key Terms:	Mentor Development Goals
➔ Introduce BEAM and learn everyone's names! ➔ **Language -** The way that humans, animals, or anything that sends and receives information in order to communicate ➔ **Code -** A system of words, letters, figures, or other symbols substituted for other words, letters, or symbols, especially for the purposes of secrecy ➔ **Cipher -** The act of disguising a written message through a series of well defined steps	● Utilize this week as trial and error. ● Develop a structure for the site each week. ● Get to really know the kids!

Mentor Development Notes
Written by Cammie Young

Teaching

Focus on developing an overall structure for the site. As this is the first week of sites for the semester, it is important that you utilize this week to establish how a site will look like on a weekly basis. Check out our virtual site guide [here](). Make sure to have a discussion with your site leaders to determine what tools or resources your site will utilize. For example, you can use the presentation templates developed by Curriculum to see what you like about it and what you want to add next time.

Don't repeat what is already on the slide! Less words, more pictures! Zoom fatigue is real, and oftentimes people won't want to listen to something that is already on a slide. Try to use examples relatable to the kids! Elaborate on details on the slides, pull up pictures, ask questions, and use hand gestures!

Pose a challenge in the beginning! A good way to start off the lesson or gauge their interest is to introduce the lesson with an activity that they don't know the answer to. The lesson ends with a cipher activity, so why not give them a hard "Crack the code" challenge at the beginning of the site to stimulate their interest so they are more likely to listen till the end.

Utilize breakout rooms on Zoom depending on the size of your site! Have your site leader create breakout rooms with one mentor in each room! Even if you have a small site, you can still use breakout rooms since it may help foster a stronger bond between you and your mentees! In these breakout rooms, check in with them regarding the content of the lesson and what they don't understand. If there's extra time, cut the ice by making small talk!

Classroom Management

Get familiar with your mentees! The main goal of the first lesson is not to hammer the concepts into the kids but really to help you foster trust and respect in your relationship with your mentees. Think of it as an investment!

A Possible Difficult Situation

The activities of this lesson assumes that everyone knows the English language. What should you do if one of your mentees can't speak or read English?
Fear not! Cryptography is essentially a form of secret communication, so if your mentee can't read or speak English, you can use another version of the cipher to help them get to code. The cipher on this website, https://thestemlaboratory.com/crack-the-code/, relates letters to pictures, so even if your mentee doesn't know English, they might understand the icons and then be able to relate it to the letters. This can help them get to the code!

Background for Mentors: Module 0

Tools	For this module we will be using **Google Jamboard** as a collaborative whiteboard space to let our mentees express themselves! You can check it out in the links in the sidebar. This space is very versatile and in addition to text and drawings, you can also place sticky notes, images, and shapes. Mentees will be using this space and the media mentioned previously to display what they think science and engineering are. Make sure to briefly go over the available tools with your mentees before they get started.
● [Google Jamboard](#) ● Zoom	
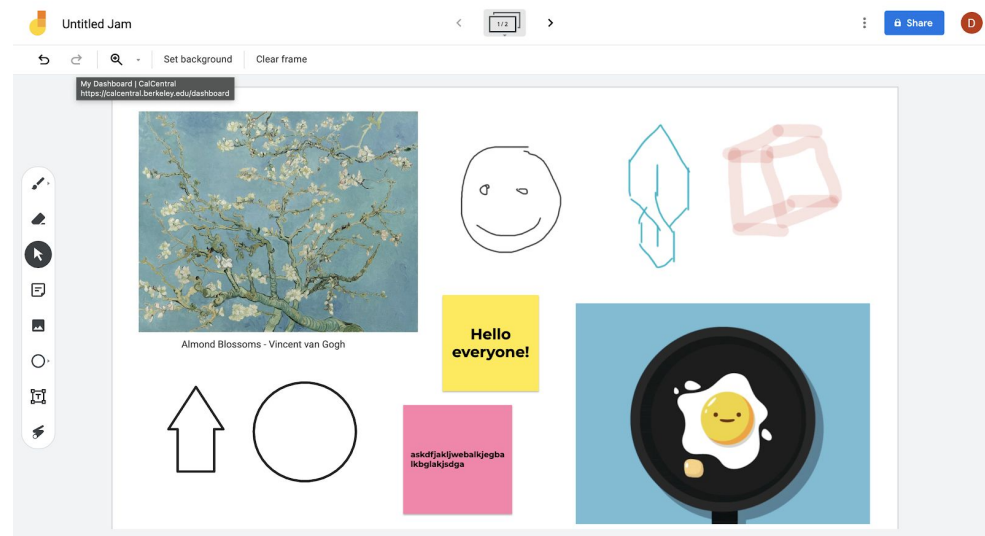
Figures 1: *An example Google Jamboard.*

On the left hand side of the screen you will find the digital tools available at your disposal: pens, image search, text boxes, sticky notes, shapes, and more. The controls at the top center of the screen let you add more boards to your project.

We are also making extensive use of **Zoom** for this lesson and the rest of the semester. Please make sure you know how to use Zoom's features such as screen sharing, polling, breakout rooms, and reactions, as these will greatly enhance your site's experience and make for an overall smoother and more fun semester. For more information, please check out these [tips and tricks](#) for educating over Zoom.

Background for Mentors: Module 1

Teaching Goals	
Teaching Goals ● Language: ○ Writing ○ Speech ○ Gesture ● Code ● Spoken Code	**Language** is the way that humans, animals, or anything that sends and receives information in order to communicate. This can come in many forms, including **written** (words, numbers, and symbols), verbal **speech**, and visual **gestures** (American Sign Language). **Figures 1 & 2:** *Hieroglyphics are a form of written language, and American Sign Language uses visual gestures to communicate* Games such as *Charades* or *Apples to Apples* take away our main form of communication and force us to refer to a secondary form, such as visual gestures and written symbols. In these cases, we are forced to guess the true meaning. Nowadays, the word "code" is usually used to refer to computer programming and the way that computers are given commands to execute. However, this definition of code comes from a more broad definition that covers all forms of language. This definition of **code** is a system of words, letters, figures, or other symbols substituted for other words, letters, or symbols, for purposes such as secrecy or when aural communication will not suffice. **Figure 3:** *Flag Semaphore uses coded visual signals to communicate over long distances* **Spoken code** is a way of sending a secret, or coded, message that uses word of mouth. The goal is to send information so that only the sender and receiver of the information understand the meaning behind the messages. During World War II, the United States Marines used Navajo Code Talkers to send verbal messages over the phone or radio. These Code Talkers used spoken code that was never broken by the enemy during the war.

Background for Mentors: Module 2

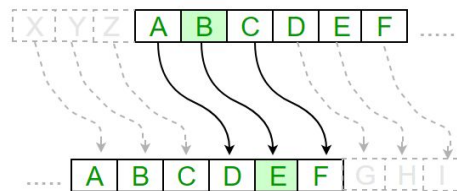| Teaching Goals	
- Cipher - The Caesar Cipher - Encode - Decode	To **cipher** is to disguise a written message in a series of well-defined steps. This makes it difficult to read, unless the reader understands the secret transcription or translation to the code. During World War II, the German army used a cipher device called the Enigma. This cipher involved a series gears that changed the letters of the message, and would change with each key press. This served to increase the difficulty of breaking the code, as successive presses of the same letter would not be converted to the same letter when coded by the enigma machine. Furthermore, the gears were interchangeable and could be swapped out in between days, only serving to add to the complexity of cracking the code. Eventually, the code was cracked by English mathematician Alan Turing, a huge breakthrough that was a huge factor in the eventual victory over Germany. **Figure 4:** *An open enigma machine with the gears visible* Another well known cipher was the **Caesar Cipher**, used by Julius Caesar, the emperor of Rome from 46-44 BC. This simple (but effective at the time) cipher used key shifts to change the letters of a message. For example, when using a 10-key shift, the letter "A" would become "K", and the letter "X" would become "H". The word "cipher" would be converted to "mszrob". **Figure 5:** *The Caesar Cipher with a 3-key shift* The act of converting information into a particular form, particularly to hide the meaning of the information (as in the case of a cipher) is known as **encoding**. The reverse form, **decoding**, involves converting the coded language back into a readable or understandable language.

Introduction

Concepts to Introduce	Questions to Pique Interest
- Language is the way we communicate with one another. What if you don't want others knowing what you're saying? - Encoding is a way to disguise the meaning behind a message, using a code, or translation. Morse code is a common example, but is not used to disguise language because it is known by many people. - Ciphers allow us to encode and decode messages. If you hope to disguise the message, only the message writer and intended message receiver should know how the cipher works.	- How would you send a secret message to your friend? - How would you create a language that only you could understand? - Why is it necessary to keep passwords secret, and what do they protect? - Prepare an encoded message before site and ask them if they can read it, explain that it has been encrypted, and at the end of the lesson they will be able to decipher it.
Scientists, Current and Past Events	**Careers and Applications**
- In 1941, Alan Turing, a mathematician, and his team cracked Nazi Germany's Enigma machine, shortening WWII by an estimated 2 years! ~70 years later, Paul Hilfinger torments CS61B students with the same Enigma machine. - Our data has to be encrypted both online and offline in order to protect it from attackers. We use a variety of encryption methods to achieve this. One of these, AES-256, would take 27 trillion trillion trillion trillion trillion years to crack by brute force with your average laptop.	- Security engineers are responsible for protecting networks and systems that can hold your data from hackers. - By creating complex passwords, we decrease the chance of our accounts being compromised, however, with computing power ever increasing, we now have additional methods such as CAPTCHAs and 2-factor authentication.

Module 0: Tell Me You're a Scientist Without Telling Me You're a Scientist

Time to meet your mentees! Begin the semester by playing an icebreaker over Zoom to help learn everyone's names.

Teaching Goals	Materials/Links
1. Introduce BEAM and learn everyone's names! **MD Goals** ● First impressions matter! Make sure that you give the mentees your undivided attention!	● Google Jamboard ○ Miro Whiteboard *(alternative if Jamboard is unaccessible)* ● Zoom Name Games

Procedure

1. Introduce yourselves and what BEAM is! Ask them some introductory questions!
   a. For this section, give mentees 5-10 minutes to add drawings, images, or text, of what they think engineers and engineering are onto a Google Jamboard. If your site is unfamiliar with this platform, take a couple of minutes to walk them through how to use it.
   b. Afterwards, go through the items on the board! Have them individually explain why they added them and what engineering and science mean to them.
   c. Take a screenshot of the board, we'll be sharing these later in decal!

2. Play a name game to familiarize yourselves with your students. We'll be teaching in a different environment for the rest of the semester, so feel free to pick an activity from this list of Zoom-friendly ice breaker games.

Example Questions:
1. What is BEAM? What do the letters in BEAM stand for?
2. What is engineering, what do engineers do? What are some things made by engineers?

Example Introduction:
   I'm a Computer Science Major and something cool I've done in my studies is create my own phone apps!

Classroom Notes

Try to encourage mentees to turn their cameras on if they are able to. If you are having trouble with giving mentees access to the Google Jamboard, you can use Miro Whiteboard as an alternative, which requires no login information. Also have the links ready to copy and paste into the chat to save time!

Module 1: Shhh Keep it a Secret

In this module students will try to "crack" the key behind a secret way of communicating chosen by the host!

Teaching Goals	Materials/Links

1. **Language -** The way that humans, animals, or anything that sends and receives information in order to communicate
    a. *Writing -* Visual text
    b. *Speech -* Verbal spoken language
    c. *Gesture -* Visual body language
 2. **Code -** A system of words, letters, figures, or other symbols substituted for other words, letters, or symbols, especially for the purposes of secrecy
 3. **Spoken Code -** a way of sending a secret message that uses word of mouth
	● *None*

Procedure

1. Explain what exactly language is, its different forms, and the meanings of "code" and what it means to use "spoken code".
2. Begin the game by explaining to mentees that they will have to attempt to join a party by bringing a valid item to your party. In order to be valid, the item that one brings must follow a secret pattern, or rule, that the "host" comes up with. This is similar to trying to break, or understand, a form of spoken code.
3. Divide the class into **breakout rooms of 3-5 mentees**, placing a mentor in each one. If your site is on the smaller side, you can skip this step.
4. The person "hosting the party" (a.k.a. the person who creates the rule), begins by saying, "*I'm having a party, and I'm bringing [item].*"
5. From there, go in a circle, and other people will try to guess the rule and bring an item that follows the rule by saying, "*I'm going to your party, and I'm bringing [item].*" Repeat items are not allowed. The host then says "*You can/can't come to my party.*" based on whether the item follows the rule.
6. If a mentee thinks they know the rule, they can

Example:

Host: "I'm having a party, and I'm bringing **apple juice**."
Person 1: "I'm going to your party, and I'm bringing **oranges**."
Host: "You **can't** come to my party."
Person 2: "I'm going to your party, and I'm bringing **water**."
Host: "You **can't** come to my party."
Person 3: "I'm going to your party, and I'm bringing a **basketball**."
Host: "You **can** come to my party."
Host: "I'm having a party, and I'm bringing **pillows**."
Person 1: "I'm going to your party, and I'm bringing a **lightbulb**."
Host: "You **can't** come to my party."
Person 2: "I'm going to your party, and I'm bringing a **tree**."
Host: "You **can** come to my party."
Person 3: "I'm going to your party, and I'm bringing **glasses**."
Host: "You **can** come to my party."

In this case, the rule is that items must have **double letters**. Other potential rules could include words that end with an "e", have exactly 5 letters,

say that they think they know the rule.

begin and end with the same letter, or words that begin with one of the letters in PARTY.

7. **Important! However, nobody is allowed to say the rule for getting into the party until everyone has gotten it.**
8. Keep going around, repeating people, even if they know what the rule is. They should be able to give examples of other items they can bring to the party in order to help out those who haven't figured out the rule.
9. Once everyone has figured out the rule, have someone else play as the party host, using their own secret rule.

Classroom Notes

Encourage mentees to make rules that are on the simpler side, otherwise the module may run long, or not enough people will be able to play as the party host. Additionally, overly complicated rules could lead to frustration!

Module 2: Ciphers

In this module, mentees will learn about ciphers and how they can be used to scramble messages. This will allow them to unscramble messages, and even write their own secret messages!

Teaching Goals	Materials
1. **Cipher -** The act of disguising a written message through a series of well-defined steps a. **The Caesar Cipher -** A certain form of cipher wherein each letter is shifted over a certain number of positions in the alphabet 2. **Encode/Decoding -** converting information to a form that disguises it and converting it back into its readable form respectively.	● [Caesar Cipher Wheel](#) ● [Pigpen Cipher Key](#) ● Blank piece of paper ● Pen or pencil
MD Tips ● Utilize breakout rooms in this section since it might get a little confusing for the kids.	

Procedure

1. Explain what ciphers are, and demo the mechanics of the online Caesar Cipher, explaining what it means to encode and decode messages using a cipher. Alternative: Pigpen Ciphers. If you are attending a middle school site, be sure to familiarize yourself with this cipher!

2. Present mentees an encoded message and have them begin to decode it, using the online Caesar Cipher linked in the materials. They should write down the message as they decode letter-by-letter. Mentees should begin by translating the message with a 1-key shift. If the first few letters don't make sense, they should start to translate the message using a 2-key shift, and continue until they find a message that makes sense.

3. If time permits, have students take turns encrypting their own message and share them in the chat along with the key. As they share these messages, lead the site in decrypting them and discovering what they say!
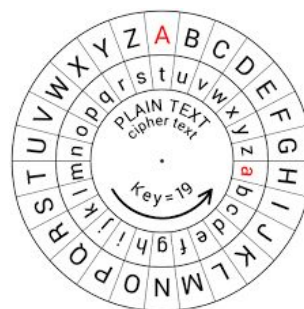

Figure 1: *The Caesar cipher with a 19-key shift, where "A" becomes "T"*

Example message: "N qtaj GJFR" is "I love BEAM" with a 5-key shift, and "Akqmvkm qa kwwt" is "Science is cool" with an 8-key shift.

Classroom Notes

Make sure the provided encrypted message is shifted by too many keys! Keep it within the 1-5 range to prevent any frustration or boredom with this module.

Conclusion

As you wrap up, see if mentees can come up with any other examples of language and messages in the real world. Have they ever played a game where they had to nonverbally act out a message? Can they name a time where they had to read symbols in the real world? Road signs and other safety signs are a great example of this.

References

- 158,962,555,217,826,360,000 (Enigma Machine) - Numberphile, Youtube
  https://www.youtube.com/watch?v=G2_Q9FoD-oQ
- Flaw in the Enigma Code - Numberphile, Youtube
  https://www.youtube.com/watch?v=V4V2bpZlqx8
- Caesar Cipher, https://www.dcode.fr/caesar-cipher
- Navajo Code Talkers, azcentral
  https://www.azcentral.com/story/news/local/arizona/2018/07/11/navajo-code-talker-facts-unbreakable-code/460262002/
- CS 161: Computer Security, University of California at Berkeley, https://cs161.org/

Summary Materials Table

Material	Amount per Site	Expected $$	Vendor (or online link)
Paper	1 sheet per student		
Pen or pencil	1 per student		