STEM core
STEM Careers through Outreach, Research, & Education

UNIVERSITY OF OREGON

Encryption, Secret Messages, and Hackers

Andrew Blaikie

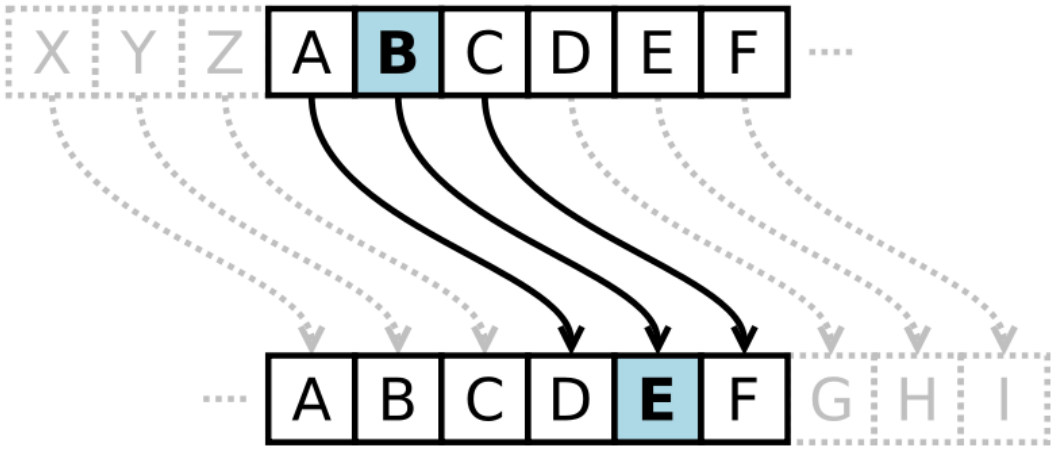
Synopsis of the Activity: The activity will have participants use the Caesar cipher encryption scheme to send secret messages to each other. The key to unlocking this message is a number between 1 and 25 (e.g. the shift in the alphabet). After messages have been sent and decrypted we will learn how this method can be hacked. I will prepare a message for them that they can try to hack (a,e, t, are used most often and this fact helps to break the code). The cipher tools will be provided to make the encryption go smoothly.

Big Idea: Provide a clear and understandable example of an encryption scheme. In the process students are learning about information theory and statistics without knowing it. Encryption plays a large role in everyday life through privacy concerns.

Audience: Middle school or late elementary school. This type of activity is best for a captive audience. It could work on a table top as well but would probably require visitors spend a good deal of time at the table. Not more than 8 participants at a time.

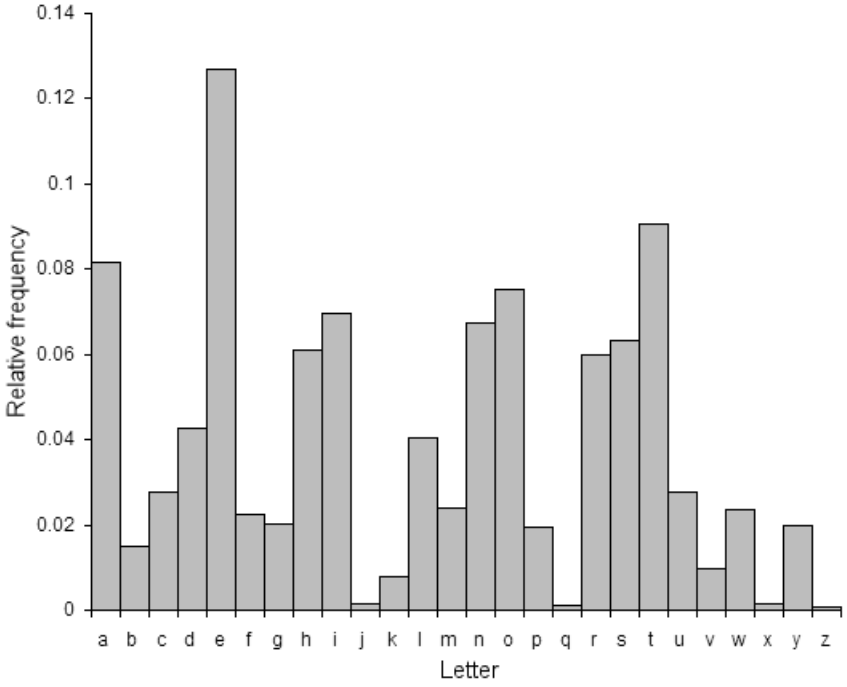
Activity (Learning) Goals OR **Learning Objectives**:

- Participants will be able to encrypt a message using a Caesar cipher (translate English to code)



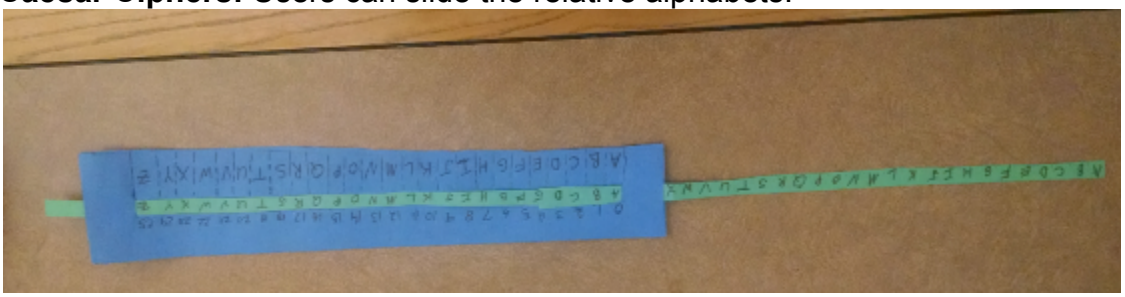
- Participants will be able to decrypt a message if they know the alphabet shift key (translate code to English)
- Participants will be able to appreciate that a code looks like gibberish if they do not know the shift.
- Participants will understand how a signature in the encryption scheme can compromise the strength of the encryption. Or alternatively a signature can help them crack a code.
- Participants will be able to use frequency analysis to crack the Caesar cipher by exploiting the signature of the English language letter frequencies (a, e, t used more often than other letters)

- Participants will gain a sense of being a scientist by going through the activities themselves
- Participants will be given an opportunity for creativity by designing their own encryption scheme

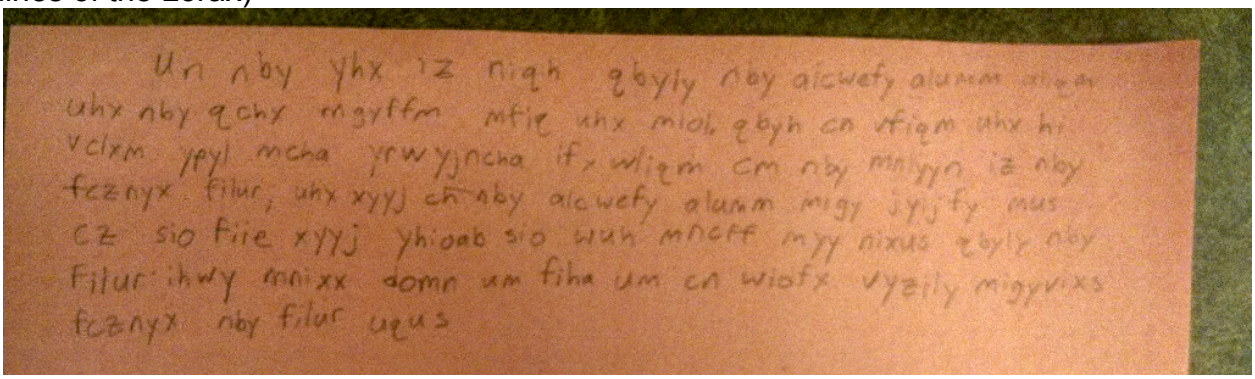


Materials:

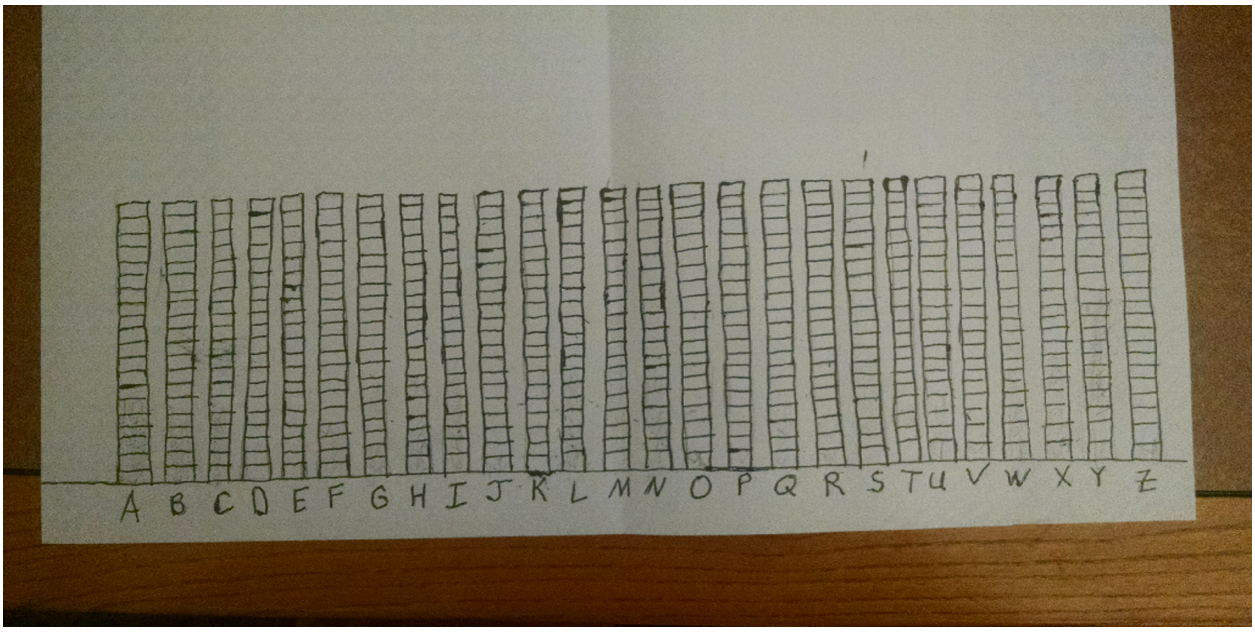
Caesar Ciphers: Users can slide the relative alphabets.



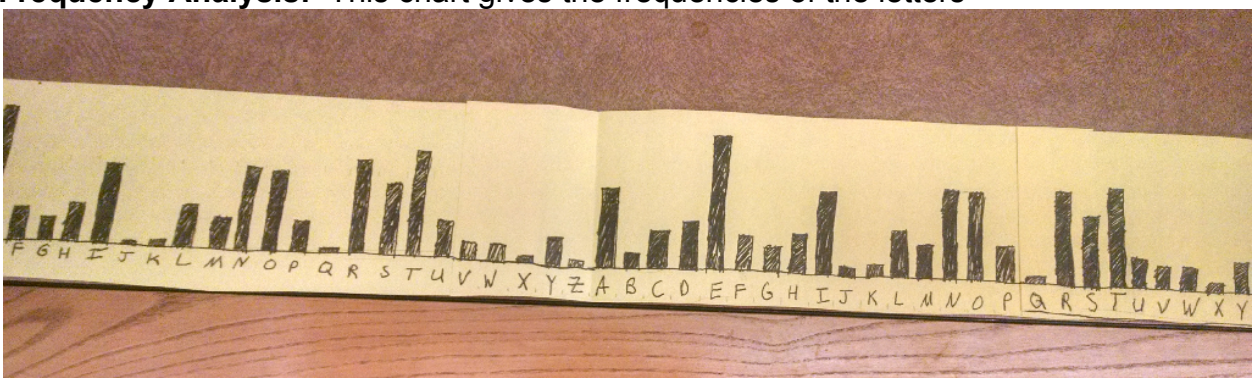
Secret Message: This is the message that I have prepared for them to crack (the first lines of the Lorax)



Histogram: Have the students mark in check boxes every time they see a letter in the code.



Frequency Analysis: This chart gives the frequencies of the letters

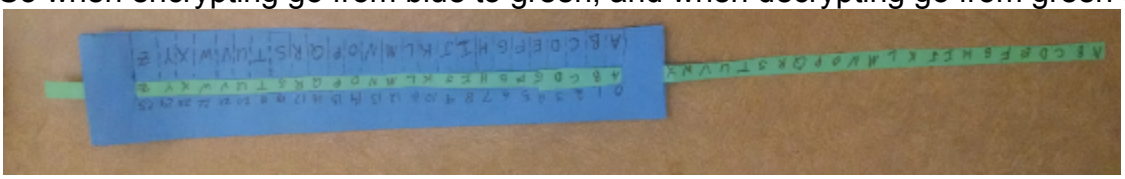


Preparation and Set-up: You will need to write your secret message for the class to decrypt. Erase the previous checked boxes in the histogram (see above picture with checked boxes)

Guiding Questions:
If I wanted to send a secret message to a friend but I knew my parents were going to look at it first how could I make it where my parents couldn't read it but my friend could?
If I were the parents and I wanted to crack the code what could I try?
How could we make this encryption more secure?

Evaluation Questions:
How would this work in a different language?
What must people do in advance before sending secret messages? (Distribute keys)

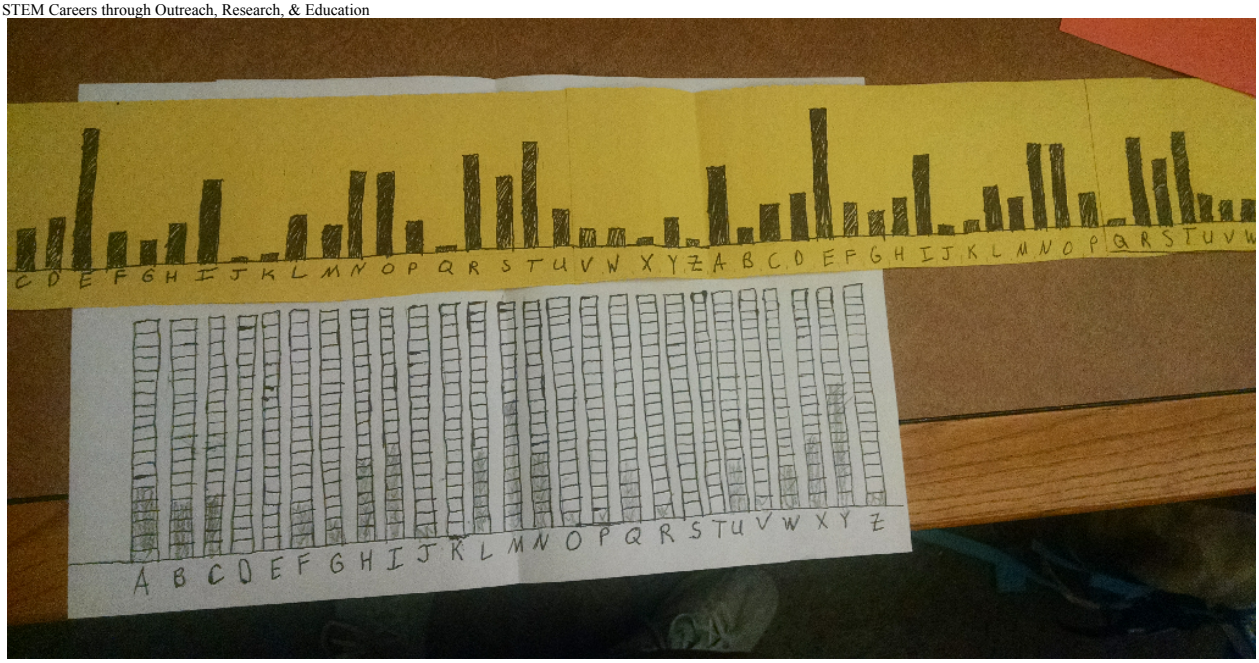
Activity Description:
Description 1: 5 minutes
Ask guiding questions to get the participants to understand how the mechanics of the Caesar cipher works and why it is useful. Be sure to explain that when using the sliders the blue letters are what you mean in English and the green letters are what is in code. So when encrypting go from blue to green, and when decrypting go from green to blue.



Phase 1: 15 minutes
In the first step everyone will write a message (a few words, like "the British are coming"), then pick a number and encrypt it. Then have trade with someone else before telling them your number. Everyone should then see that the message looks like gibberish) Example: "The British are coming"-> "ymj gwnynxm fwj htrnsl" with a shift of 6. Then trade keys and then decrypt your partner's message.

Description 2: 5 minutes
See if any of the students have ideas on how to crack a message where you do not know the shift. Ask leading questions to get them to see that certain letters are used more than others. Then give them the letter frequency chart to study.

Phase 2: 15 minutes
I give the class all copies of a message I have "intercepted" that needs to be cracked as soon as possible. Give the group the check box histogram so they can tally up the total time each letter is used. Then slide the signature until the probabilities match up. Tell them to focus on the letters A, E, T, and the least common letters Q, X, Z, J. Hopefully they can then crack the code! Here is my Example



Teaching Strategies:
Engagement: Secret messages are cool! Preface activity with real world example like how the German code was cracked during World War 2 and the American code was not. Ask why someone might want to send a secret message (financial transactions and internet privacy is a big modern example).

Exploration: Everyone gets to choose their own key and write their own message. Furthermore everyone gets to try to crack the code (with guidance).

Explanation: Ask debriefing questions to see if the participants understood the exercises. I found that some participants needed to see me encrypt a message before they understood how it worked and then they could do it themselves afterwards.

Extension: If more time have the student's try to think of their own encryption scheme that is more secure than the one we practiced. See if anyone comes up with anything creative! If drawing blanks you could introduce them to the polyalphabetic cipher (see khan academy link).

Evaluation: Were they able to understand the mechanics, relevance, and opportunity for further exploration within this demo?

Vocabulary:
Encryption->translate message to code
Decryption->change code back to message
Key-> knowledge used to go from message to code
Signature-> any weaknesses in the code that allows it to be hacked

Science Content Background and Additional Resources:

https://www.khanacademy.org/computing/computer-science/cryptography

http://en.wikipedia.org/wiki/Caesar_cipher