Cryptography: The Math of Secrets

Learning Objectives
Students will be able to:

- Describe what cryptography is and how it has been used throughout history, as well as **key terminology** such as encrypt, decrypt, frequency graph, code, cipher, Caesar cipher, modular arithmetic.
- Apply a Caesar Cipher to a message and use frequency analysis to crack a Caesar cipher.
- Appreciate math as the study of patterns.
- Name the contributions of early female cryptographers and codebreakers.

Materials:

- Student Handout
- Caesar Cipher wheels printable
- Paper fasteners
- Scissors
- Markers
- White Boards
- White Board markers
- Graph paper

Motivation (5 min)
Who's ever wanted to learn to pick locks? Send secret messages?

- Codes and ciphers are virtual locks
- Instead of putting information into a locked box, we change the information so it can't be easily read

When would a code or a cipher be useful? (Have students write ideas individually on white boards)

- Thousands of talented women were secretly recruited and trained during the war to become codebreakers for the US Army and Navy. Working tirelessly at two codebreaking centers in the DC area, these women cracked code that provided critical intelligence information in the European and Pacific Theaters.
- Read more in *Code Girls* by Liza Mundy

ABC Cipher
Group Brainstorm (5 min) – *Ask the following questions and take answers from the group.*

- What are ways you could **encrypt** a message?
    - Scramble the letters
    - Assign letters to new letters.
    - We call these techniques ciphers

        - Codes and ciphers are forms of secret communication. A code replaces words, phrases, or sentences with groups of letters or numbers, while a cipher rearranges letters or uses substitutes to disguise the message.

Example (10 min) - *Have each student encrypt "Femme in STEM" using an ABC cipher*

- On their whiteboards, have each student write out the alphabet and their encryption below it
    - They should each get something different in the end

Summary (3 min) - How could we make this better?

- Something that is harder to crack (or "**decrypt**") is a better cipher
- Point out that each time you want to change the cipher, you would have to agree on a whole new alphabet scheme together.

Caesar Cipher

Intro Discussion (2 min)

- Who's heard of Julius Caesar before? (Roman leader/politician/military 100-44 BC)
    - Julius Caesar used to send messages to his soldiers using an improved technique that we now call the Caesar Cipher. He wanted the messages to appear meaningless if they were intercepted.
- The Caesar Cipher and the ABC Cipher are **Substitution Ciphers** because you substitute one letter for another

Caesar Cipher Wheels

Have students explore pre-made Caesar Wheels (see Student Handout). (1 min)

The Caesar Cipher is a more organized ABC Cipher.

- Instead of needing to agree on an entire layout of the alphabet, I can just tell you "+3" and you would have all the info needed to decrypt
- This very basic cipher was used for hundreds of years after Caesar.

Practice (9 min)

- Encrypt STEMinism using a +7 shift
- Encrypt Cryptography using a -17 shift
- Decrypt mymxfxjhwjy (It is a secret) using a +5 shift
- RACE! Decrypt uxahqymft (I love math) using a +12 shift

Modular Arithmetic (25 min)

What if you lost your wheel? You can do the same process by assigning a number to each letter and then adding the shift

- This is called **modular arithmetic.** It works the same why clocks do. You decide all multiples of a number will be the same as 0 and then you figure out "how far away" are you from the last multiple
    - Explore modular arithmetic with the usual number system.

- What if your shift is +15 and you need to encrypt the letter t = 20? Which letter =35?

A b c d e f g h i j k l m n o p q r s t u v w x y z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Cryptography Today -- Discussion, take answers (10 min)

- What would we want to encode today? Where do we use cryptography in our lives?
- What other ciphers exist?
    - Hedy Lamarr - actress during WWII who came up with the idea of "frequency hopping." This encrypted the radio signals of ships and submarines, instead of information
        - Basis for bluetooth

Breaking Substitution Ciphers

Intro Discussion (5 min)

What would you do if you didn't know what the Caesar Cipher shift was? How would you crack the message? (Take ideas).

A lock is only as strong as its weakest point. A lock breaker might look for mechanical weak points. The method to break a Caesar Cipher wasn't written down until 800 years later by an Arab mathematician named Al-Kindi.

- He broke the Caesar Cipher by finding an important clue about the language a message is written in - letters aren't used with the same frequency.

Who knows what letter is used most often in English? Who thinks all letters are used the same amount? Let's figure it out.

Frequency Graph (30 min)

Distribute the following passage:

Mr. and Mrs. Dursley of number four, Privet Drive were proud to say they were perfectly normal, thank you very much. They were the last people you'd expect to be involved in anything strange or mysterious, because they just didn't hold with such nonsense. Mr. Dursley was the director of a firm called Grunnings, which made drills. He was a big, beefy man with hardly any neck, although he did have a very large mustache. Mrs. Dursley was thin and blonde and had nearly twice the usual amount of neck, which came in very useful as she spent so much of her time craning over garden fences, spying on the neighbors.

Have students pick a few letters and count how often it appears. Together, they can put together a frequency graph - a bar chart that shows how often each letter appeared in the passage.

Questions to ask:

- Now if we know “e” and “t” are the most common letters in English, and “p” and “q” are the most common letters in our encrypted passage, what could we do when trying to decrypt the message?
- “J” and “z” are the least common letters. What about if we saw “a” and “l” are the least common letters?
- How do we know our information is an accurate representation of the English language?
-

Work together to create another frequency chart for the encrypted message:
Gipko kxdc cik tipki xniprig cdaf udko wdvcepc w dvepsi hiifpqq ixcig pc edm tpkcr rqe ddn du tacqe qkpuc pfgt abpk gkw xnipriu afg ifqnd rigp narc dupnn fiqirr pkw hddlrpfg ijva xoifc ciko him afrdfr ixcio hik dfiti ptpac wdvk dtn hw fd npcik cepf yvnw ceakcw uakrc wdvkr rafqikinw oafiksp oqmdfpmpnn

Compare the frequency charts. Use them to decrypt the message.
Decrypted Message: Dear Mr potter we are pleased to inform you that you have been accepted at hogwarts school of witchcraft and wizardry please find enclosed a list of all necessary books and equipment term begins on september one we await your owl by no later than july thirty first yours sincerely minerva mcgonagall

Science Fair
- Have students describe the Caesar Cipher and how it works
    - Have them help peers encrypt and decrypt a few messages (generated by the math students) using their wheels
- Have students describe how to break a Caesar Cipher using frequency analysis
    - They will have to define frequency analysis

***Extra:** If extra time, have students encrypt messages in groups, swap, and race to use their frequency charts to break the code.

Summary
Why did we do this activity in the math group?
What do you think math is?
- Math is the search for patterns. Mathematicians look for or create patterns to describe what is going on around them.
- Here we used patterns in language to crack codes.

Things to Discuss During the Activity:
- Number Theory - a branch of mathematics that studies integers (the counting numbers)
    - Cryptography is studied by number theorists
    - Number theorists are very interested in looking for prime numbers
        - This also has to do with cryptography. More complicated ciphers rely on patterns that are much harder to find. Prime numbers are very hard to find

- we haven't figured out the pattern that tells us how often they occur yet. So basing a cipher on prime numbers is pretty strong
    - This is how online encryption works, like if you buy something or any online banking
- Probability Theory - a branch of mathematics that studies possibilities
    - They like to make predictions about the likelihood something will happen based on frequency data - just like we did!
- Code Girls - Book about the women cryptographers in WWII. Over half the cryptographers were women - astounding for the time.
- Hedy Lamarr - actress during WWII who came up with the idea of "frequency hopping." This encrypted the radio signals of ships and submarines, instead of information
    - Basis for bluetooth