Cyber Security

Keeping your information safe

<u>Standards:</u> (Core ideas related to the activity)

NGSS:

ETS1.B – A solution needs to be tested and them modified on the basis of the test results in order to improve it

MS-PS4.C – Digitized signals sent as wave pulses are a more reliable way to encode and transmit information

CC Math:

5.OA-3 – Analyze patterns and relationships

K12CS:

3-5 CS-Devices – Computing devices may be connected to other devices or components to extend their capabilities. Connections can take many forms such as physical or wireless.

3-5 N&I-Cybersecurity – Information can be protected using various security measures. These measures can be physical or digital

3-5 IoC-Culture – The development and modification of computing technology is driven by people's needs and wants and can affect different groups differently

6-8 CS-Devices – The interaction between humans and computing devices presents advantages, disadvantages, and unintended consequences. The study of human-computer interaction can improve the design of devices and extend the abilities of humans.

6-8 N&I-Cybersecurity – The information sent and received across networks can be protected from unauthorized access and modification in a variety of ways, such as encryption to maintain its confidentiality and restricted access to maintain its integrity. Security measures to safeguard online information proactively address the threat of breaches to personal and private data

6-8 A&P-Algorithms – Algorithms affect how people interact with computers and the way computers respond. People design algorithms that are generalizable to many situations

6-8 IoC-Culture – Advancements in computing technology change people's everyday activities. Society is faced with tradeoffs due to the increasing globalization and automation that computing brings

Objectives:

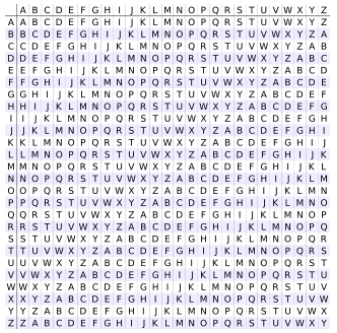
The students will:

1. Discuss the history of keeping information secret and relate it to the need for online privacy today.
2. Define and implement several different kinds of cipher techniques.

Background:

People have been sending secret messages since the beginning of written messages. **Cryptography** literally means 'secret writing' and is the word we use for methods used to create secret messages. From the very beginning simple **substitution ciphers** were used to **encrypt** messages before they were sent. These substitutions depended on the receiver of the message having a **key** to tell them what the substitutions were so that they could **decrypt** the messages upon arrival.

During ancient Greek and Roman times, advances in cryptography included the scytale (rhymes with Italy). These were used particularly by the Spartan military, and anyone who intercepted it would have to have a tool of exactly the correct size to read the message. Later, the Caesar cipher was invented, a form of substitution cipher that simply shifts the alphabet. The key is in that the receiver must know exactly how far and in which direction the shift occurred during encoding.



Cryptography continued to play a role in the politics and intrigue of the middle ages, depending mostly on substitution or **transposition** coding. The biggest advance was the use of an alphabet table called the Tabula Recta, used to shift the substitution several times throughout the message, a method called the Trithemius cipher. Later, Charles Babbage (coincidentally the inventer of an early computer) was able to see correlations that occur in all of these kinds of ciphers and he came up with a key to break them.

In the modern era, codes and code breaking played a huge role in both WWI and WWII. One of the main reasons the US entered the First World War was a secret message the the British intercepted and decrypted from the German government, inviting Mexico to join them in return for land in Texas, New Mexico, and Arizona. This document was known as the 'Zimmerman Telegram' and possibly changed the direction of the war.

In World War II the addition of machines to aid in encryption made code breaking much more difficult. The German 'Enigma' and 'Lorenz' machines used a sophisticated combination of electric signals and mechanical rotors to encode messages. Code breakers worked on these messages by hand at first but later, machines like the Bombe and Colossus were invented to speed the decoding process. These machines were early versions of **computers.**

Because of the use of computers, modern cryptography is much more complex, involving mathmatical theory and complex **algorithms.** Computers allow for the encryption of any kind of **data**, not just text as was the case in earlier forms of encryption. Being able to encrypt data is more important than ever, as we use computers and the internet to take care of personal items like banking and commerce, as well as medical and school records.

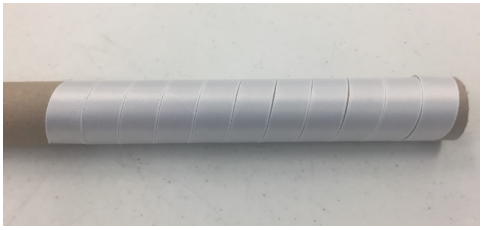
Vocabulary:

- Algorithm – a set of instructions that is followed to solve a problem or complete a procedure
- Brute Force – breaking a code without a key, most often using trial and error
- Cipher – a way to encrypt and decrypt data; they allow people to keep their information secure and secret
- Ciphertext - text that has been encrypted
- Computer – any machine that can be instructed to do a series of actions, calculations, or operations
- Cryptography – any of the methods used to create secret messages
- Data - the quantities, characters, or symbols that computers use to carry out their operations; data is stored and transmitted in the form of electrical signals
- Decrypt - restoring the data to its original readable form
- Encrypt - to make data unreadable to anyone without the key
- Key – what is used to encrypt and decrypt information
- Substitution Cipher – a cipher that replaces the letters with something else to encrypt the message
- Transposition Cipher – a cipher that rearranges the letters to encrypt the message

Supplies:

- 3 different sized tubes: *length is not important; width needs to differ between all three. Recommended: paper towel tube, various wrapping paper tubes, etc.
- Ribbon or paper easily twisted around the tubes (white works best).
- Permanent marker
- Tape
- Caesar Cypher Wheels (printed out)
- Scissors
- Split paper brads
- Cryptography Worksheet: The Scytale Cipher
- Cryptography Worksheet: Caesar Cipher
- Cryptography Worksheet: Cell Phone Cipher

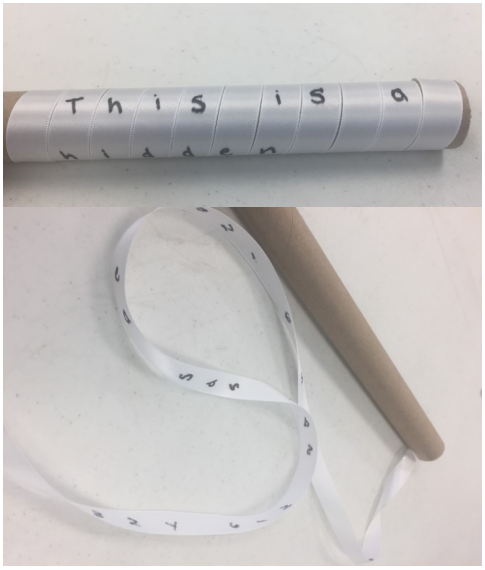
Prep:



To prep the Scytale Ciphers:

1. Grab one of the three tubes you have for this activity, and the ribbon to go on it.

2. Tape the end of the ribbon onto the end of the tube and wrap it around tightly.
3. Write your message, you can write it vertically or horizontally.
    a. Message one (first tube) should read ‘to infinity and beyond!’
    b. Message two (second tube) should read ‘twinning and winning!’
    c. Message three (third tube) should read ‘born in pasadena, ca’
4. When the ribbon is unrolled, the message will be encrypted.



Print the Caesar Cipher wheels for each group.

Procedure:

There are two main types of ciphers: substitution and transposition. Both are valid means of keeping messages and data safe, and this activity uses both.

Your students will use three methods to decrypt all of the messages and figure out which NASA mission is hidden in the clues.

Scytales (transposition)

1. If possible, split your students into groups – if not you will have to make several sets of the scytale.
2. Give students a copy of the data sheet found at the end of the lesson plan. They will use this to write all of their decoded messages.
3. Give the students a ribbon that you have encoded. Have them try to figure out what the message is. Tell them the history of the scytale and explain that the **key** to decrypting these messages is the size of the tube. Give the tubes out randomly and explain how to wrap the ribbon to read the message. Since you gave the tubes out randomly, some of the groups may still have gibberish. Help them to figure out why, and redistribute the tubes so that the messages are readable. Have the students share the messages with the rest of the class so that they can fill in their data sheet.

Caesar Ciphers (substitution)

1. Give each student a copy of the Caesar Cipher wheel (found at the end of the lesson plan). Have the students cut the two wheels out.
2. Use a pencil or pen to poke a hole through the center of the two wheels. Stack the smaller wheel on the larger wheel and use a split brad to secure them. You should be able to spin the wheels in opposite directions.

3. The Caesar Cipher starts with both the inner and outer wheels aligned. The key is how many clicks to turn the inner wheel to both encrypt and decrypt the messages. For example, if the key is 2, start with the wheels aligned, turn the inner wheel 2 clicks clockwise so that A is now Y, B is now Z, etc. The worksheet will include the key for the first three, but will encourage the students to '**brute force**' decrypt the fourth.

Cell Phone Ciphers (substitution)

1. The key to this cipher is the cell phone keypad – and the letters associated with each number. Under each number is three or four letters, and this code uses the number the letter is under as well as its position to encode. For example, A would be 2, B would be 22, and C would be 222. You can give them instructions on how this key works, or you can just tell them to use the phone keypad and see if they can break the key on their own. (Included is an image of a phone keypad to use if you don't want your students to have their phones out in class.)

Answers to worksheet:

Scytale:

1. To infinity and beyond
2. Twinning and winning
3. Born in Pasadena, CA

Caesar Cipher

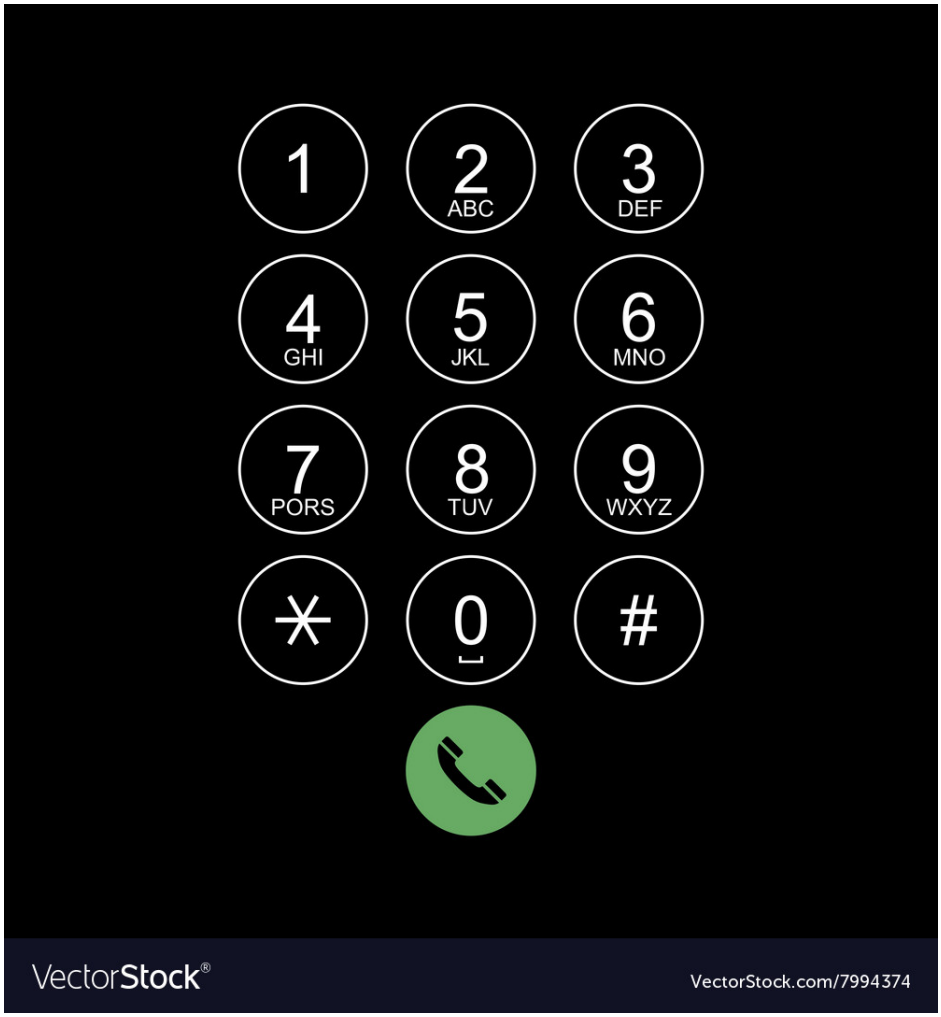
1. Forty three years and counting
2. Planetary family portrait
3. Carl Sagan is my friend
4. One goes up, one goes down

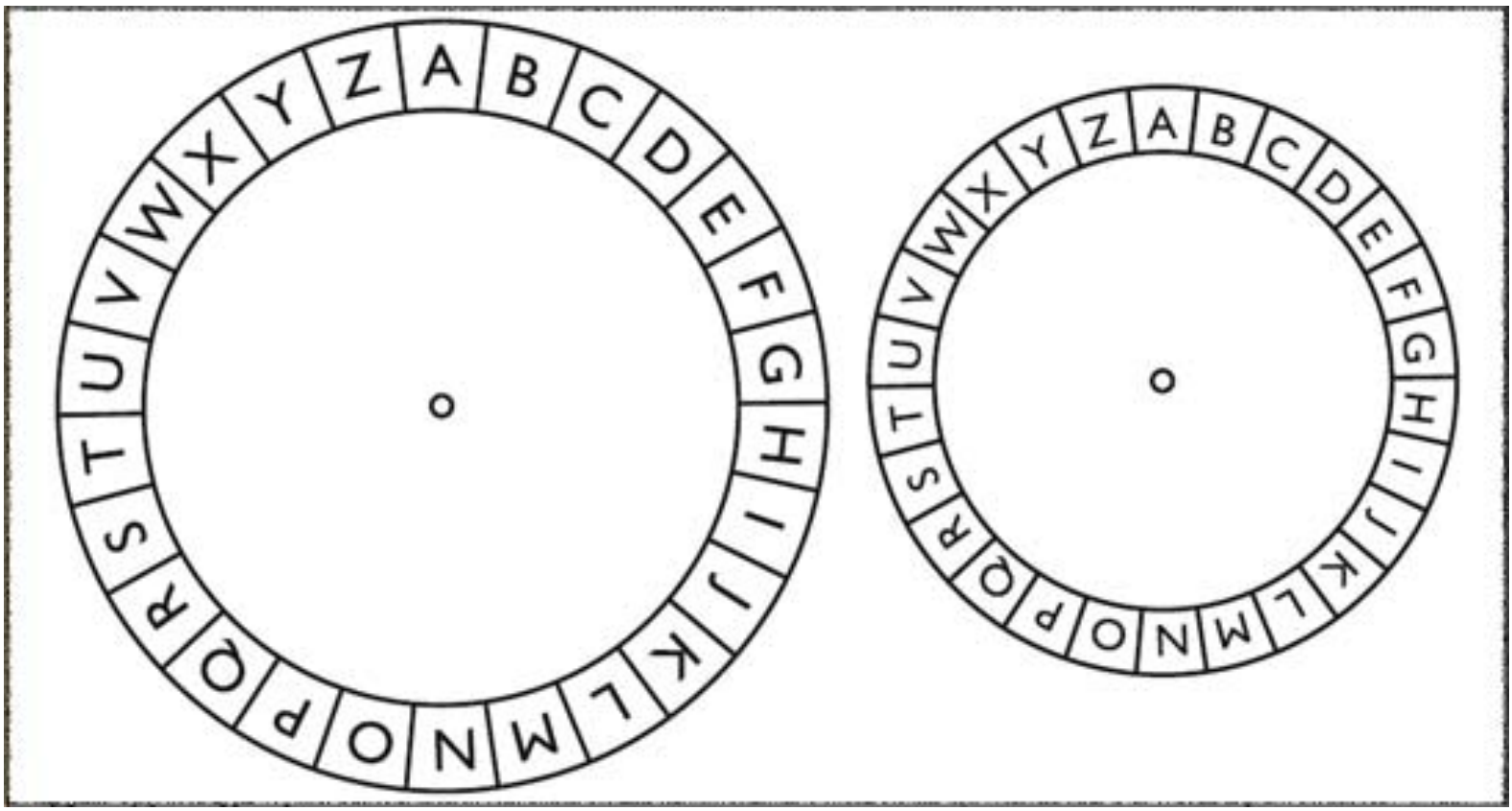
Cell Phone Cipher

1. Pale blue dot
2. Pure gold
3. Grand tour
4. Gone interstellar

NASA Mission

Voyager – NASA's mission to leave the solar system. Both spacecraft launched in 1977, going opposite directions. Voyager 1 reached interstellar space in 2012, and Voyager 2 reached interstellar space in 2018. On the way out, an exploration of the outer planets completed the Grand Tour of our solar system. Both spacecraft carry with them a golden record that contains a greeting to any intelligent life that may come across our interstellar Voyagers.
https://voyager.jpl.nasa.gov/mission/


1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PORS
8 TUV
9 WXYZ
*
0
#
VectorStock®
VectorStock.com/7994374


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
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

Credits:

Image: https://blog.cryptographyengineering.com/2012/10/09/so-you-want-to-use-alternative-cipher/

https://interestingengineering.com/charles-babbages-inventions-revolutionized-computing-and-the-world

https://www.archives.gov/education/lessons/zimmermann

https://www.thehistorypress.co.uk/articles/how-lorenz-was-different-from-enigma/

Image: https://www.vectorstock.com/royalty-free-vector/flat-keypad-for-phone-vector-7994374

Scytale Messages:

1. _____

2. _____

3. _____

Caesar Cipher Messages:

1. Key 3
   CLOQV QEOBB VBXOP XKA ZLRKQFKD!
   _____

2. Key 5
   KGVIZOVMT AVHDGT KJMOMVDO
   _____

3. Key 7
   VTKE LTZTG BL FR YKBXGW
   _____

4. Brute Force
   NMD FNDR TO, NMD FNDR CNVM
   _____

Cell Phone Cipher

1. 7-2-555-33 22-555-88-33 3-666-8
   _____

2. 7-88-777-33 4-666-555-3
   _____

3. 4-777-2-66-3 8-666-88-777

_____

4. 4-666-66-33 444-66-8-33-777-7777-8-33-555-555-2-777

_____

Final Answer:

Name the NASA mission!