Cryptography – Caesar's Cipher

This week's Looney Challenge explores **cryptography** and the **Caesar Cipher.** This Challenge compliments the 2014-2015 Looney Challenges, *Turing and Enigma* (April 16, 2015) and *Cryptography* (March 16, 2015). Go to the Looney Challenge Archives (http://ou.montana.edu/csoutreach/previous_looney-challenges.html) to find the Challenges.

The **Caesar Cipher**, also known as the *Caesar Shift*, is simple and one of the oldest known ciphers used to encrypt messages. Julius Caesar used the cipher to send messages to his generals. The cipher is a substitution cipher, where each letter (a,b,c,d…) is shifted a certain number of spaces down the alphabet. The number of spaces is known as the "key."

To introduce the Caesar Cipher, ask your students to watch *Introduction to Cryptography: Caesar Cipher*,   https://www.youtube.com/watch?v=pIt4Q68J00A.

The following vocabulary will also be useful for students to understand:

Vocabulary*:

- **Plaintext** – *The intelligible form of an encrypted text or of its elements.*
- **Ciphertext** – *The enciphered form of a text or of its elements.*
- **Encrypt** – *To change (information) from one form to another especially to hide its meaning.*
- **Cipher Disk** – An enciphering and deciphering tool developed in 1470 by Leon Battista Alberti. The device consists of two concentric circular plates mounted one on top of the other (https://en.wikipedia.org/wiki/Cipher_disk).
- **Key** – the number of "shifts" to decrypt a message (http://www.cryptoclub.org/).
- **Cipher** – *A way of changing a message to keep it secret.*
- **Substitution Cipher** – *A cipher in which the letters of the plaintext are systematically replaced by substitute letters.*

* All Definitions are from Merriam-Webster online unless otherwise noted (www.merriam-webster.com/dictionary/encrypt).

Additional Resources:

Practical Cryptography, http://practicalcryptography.com/ciphers/caesar-cipher/
Secret Code Breaker: Caesar Cipher History, http://www.secretcodebreaker.com/history2.html
Caesar Cipher, https://en.wikipedia.org/wiki/Caesar_cipher
CryptoClub: Teacher's Guide, http://www.math.uic.edu/CryptoClubProject/CCpacket.pdf - the packet contains additional activities and definitions.

Let's Get Started

Now that you have learned about the Caesar Cipher and how to encrypt a secret message, let's have some fun (10 points).

For all students (K-12):

1. The *Caesar Shift* worksheet:
   - The goal is for students to gain an understanding of the cipher and how to decrypt a message.
   - First, ask your students do a simple activity using the cryptography worksheet. Click here (http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/shift.pdf) and download the worksheet. Print as many copies as you need.

- Follow the directions, complete the table and answer the questions on page 1. Note: Teacher notes begin on page 2.
- Option – Ask your students to make a cipher disk (or wheel). Instructions and template can be found on pages 3-4.   It's up to you if you would like students to construct their own Caesar Wheel or students can access an online version on the Crypto Club webpage, http://www.cryptoclub.org/tools/caesar_cipher.php.
- You may need to adapt the worksheet to the different age levels in your classroom.
- For additional practice, you can ask students to create secret messages with a partner.

2. Ask your students to play *"Desert Oasis Treasure Hunt."*
- Go to http://www.cryptoclub.org/
- Click on "Ciphers" to link to encrypting and decrypting tools. Click on the "Caesar" button. Your students can encrypt and decrypt messages and become more comfortable with the Caesar Wheel (Cipher disk) online before playing the game.
- When you are ready, go back to the main page and click on "Games."
- Click on the "Desert Oasis" game to start playing. The game becomes more difficult as students progress.
- If students are interested, they can also play "Rogue Computer."

3. **Extra Credit (5 points)** – Ask your students to decrypt a message from Looney the Robot using the Looney Cipher. Please go to the Looney Cipher and Looney the Robot Secret Message below. Print as many copies as you need
- Beginners: Allow your students to use the cipher to decrypt the message. How did the students decrypt the message? How did the students differ in their approaches to solving the message?
- Intermediate: Provide your students with one or two "clues" to get them started. For example, ask them to identify one or two animals that occur most frequently, what "letter" do they think the animal represents? Give them 2-4 of the most frequent letters. How do the students decrypt the message using only 2-4 letters? Were they able to figure out the message? If needed, provide one or two additional letters.
- Advanced: Let the students work together or on their own without providing a "clue." How are the students solving the message? Provide clues, if needed.

How to earn points:

1) If you haven't registered your class, please go to cs.montana.edu/looney-challenge and click on the "Register for Looney Challenges" link.
2) Discuss with your class the difficulty of the activity. What did they learn? How difficult was the activity? Do they understand the concept?
3) Briefly, in a couple of sentences, describe in your email what happened during the activity? Did your students understand the concept(s)? Email your description to looneychallenges@gmail.com
4) If you want to attach an example, photographs of students working, or video of student's outcomes, please send them as an attachment.
5) We will send you a confirmation and provide you your point total for the activity and your total points for Looney Challenges.

All Looney Challenges can be completed at any time during the 2015-2016 school year. All Challenges are due, June 30, 2016.

Questions? Please send an email to looneychallenges@gmail.com or call Sharlyn Izurieta at (406) 994-4794.

DEADLINE is June 30th, 2015.

Greetings

from Looney the Robot and Hunter!

Looney, just like a groundhog, woke up on February 2nd and saw his shadow - SIX more weeks of winter in Montana! He loves snow, but is looking forward to Spring and tip-toeing through the tulips. Use Looney's Cryptograph to decode his favorite Spring quote!
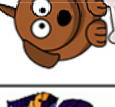
Answer: "It's a beautiful day, don't let it get away."

- Unknown Author

Looney Cryptograph

Can you encrypt a message using Looney's cipher?

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

HAVE FUN !