NAME _____ DATE _____

The Secret Code:
CAPTCHA and the Cipher disk

BACKGROUND:

"Cryptology" is the study of codes. Codes are a way of keeping data and private information secure. Codes have been used to protect national secrets, national defense, and government officials for more than 4000 years. For example, Julius Caesar used "code wheels" and the Caesar Cipher to send secret messages to his military generals in the field, fighting the enemies of Rome. Variations of the code wheel method have been used for at least 2000 years.

Today, codes are essential for protecting personal and financial information accessed on computers. Modern-day cryptology uses mathematical applications such as number theory, formulas, and algorithms for data storage and security. Building on this research, Luis von Ahn created a system that keeps access to websites that host personal information safe and secure.

MATERIALS:

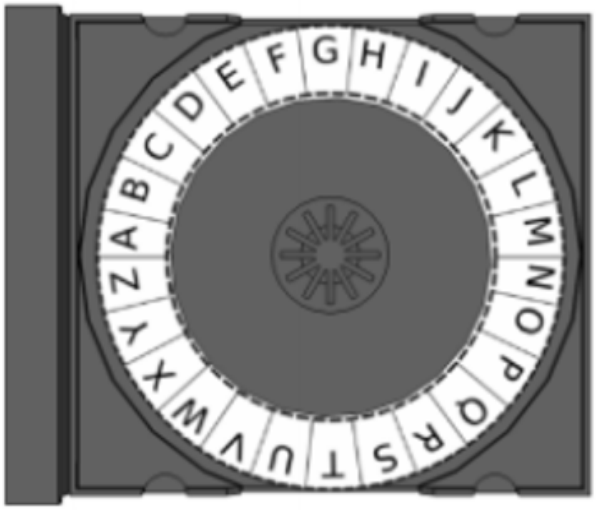
- Mini-CDs (3 inches) or equivalent-sized circle
- Media tray for standard CD
- Template labels for mini-CD and media tray

NAME _____ DATE _____

DIRECTIONS:

HOW TO BUILD A CIPHER DISC

1. Place the large ring template with letters into the CD case (Figure A).
2. Place the small ring template with letters onto the mini-CD (Figure B).
3. Place mini-CD or circle into the media tray.
4. Line up the letter A on the small circle with the letter A on the large circle.



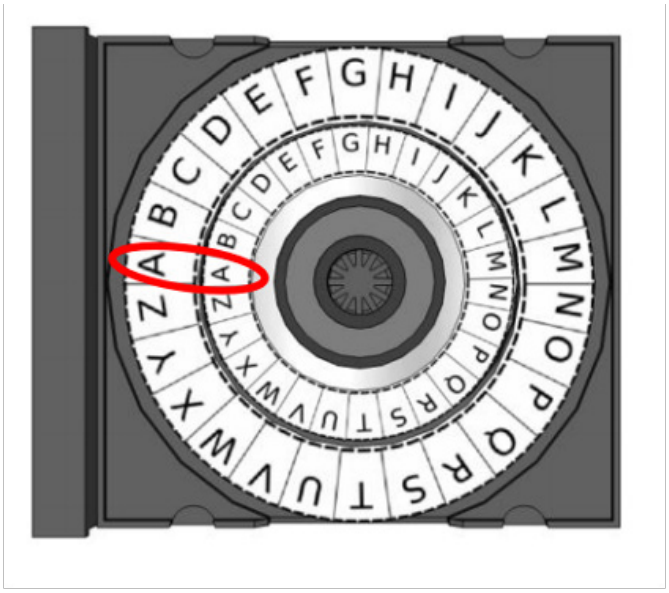
A

B

NAME _____ DATE _____

LEARNING TO USE THE CIPHER CODE WHEEL

1. The small ring has the letters you want to use to create your code of what you want to say. The large ring has the letters that will become the code.
2. Creating the code is called encoding. The phrase "key of" tells how many spaces you have to move the inner disc to determine the coded letter.
3. How do you encode HELP using the key of 3?
    a. Turn the mini-CD three positions to the right (clockwise).
    b. H on the small disc now lines up with K on the large disc.
    c. E on the small disc lines up with H on the large disc.
    d. L on the small disc lines up with O on the large disc.
    e. P on the small disc lines up with S on the large disc.
    f. Hint: HELP on the small disc becomes KHOS on the large cipher disc
    g. To ENCODE, shift the ring according to the key. Read from the inner circle to the outer circle. Create the code.
    h. To DECODE, shift the inner ring clockwise to the number of places according to the key. Read from the outer ring to the inner ring to interpret the code.



NAME _____ DATE _____

QUESTIONS:

1. Based on your encoding, what is the meaning of "key of 3?"

2. Use your Caesar Cipher to decode the following cipher text messages using the keys given. Remember to line up each A before rotating the mini-disc to decode each message.

   a. *UTRE OT ZNK JGXQTKYY, IGT EUA YKK ZNK YZGXY.*
   Martin Luther King Jr. (key of 6; move the A on the mini-CD clockwise six spaces)

   b. *NAWYPERC EJ WJCAN KNWJJKUWJYA SEHH JKP WZRWJYA KJA'O WXEHEPU PK LANOQWZA.*
   Ruth Bader Ginsburg (key of -4; for negative keys, move the mini-CD counter-clockwise four spaces)

   c. Write a code for a Luis von Ahn quote in the key of 9.
   "Every time you buy tickets on Ticketmaster, you help digitize a book."

3. Choose a positive or negative number to serve as the key. Create your own encoded message for someone else to try and decode.

OPTIONAL CHALLENGES

- Create messages with unknown encryption keys for peers to solve.
- Convert encrypted messages into binary code.
- Try to encrypt a message using the alphabet from a foreign language.
- Change the key values at specific points in the message, making it harder to decode.

NAME _____ DATE _____

ADDITIONAL MATH CONTENT FOR THIS ACTIVITY

The Caesar Cipher is a substitution cipher where the code creation uses modular arithmetic to shift the letters. **Modular arithmetic** means that numbers "wrap around" when they reach a certain point. For example, the clock works on two twelve-hour periods, AM and PM.

The hour number starts over after it goes around the clock.

The Caesar Cipher Disc works around the number of letters in the alphabet. 26 represents the number of modules.

Math expressions can represent the coding and decoding functions of the Caesar Cipher:

E (x,k) = (x+k) mod 26 D (y,k) = (y-k) mod 26

E = the encoding function

D = the decoding function

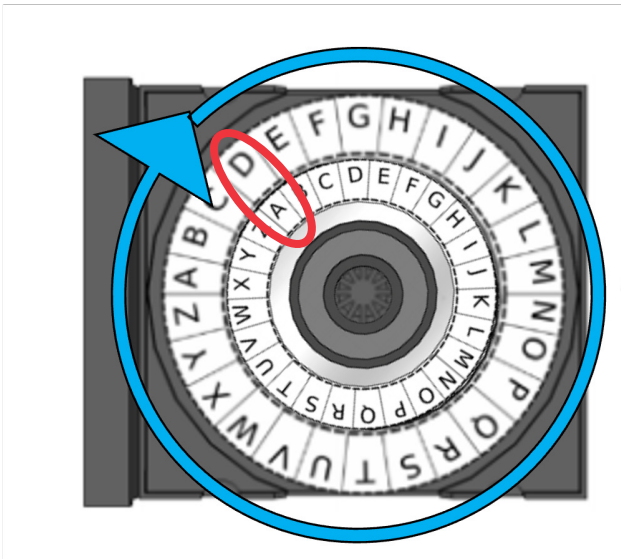
x = the small disc letter

y = the cipher text letter

k = the secret key

If x+y is greater than 26, turn the disc around 26 positions in the clockwise direction. The disc will return to the starting letter position and keep going to complete the remainder of the positions.

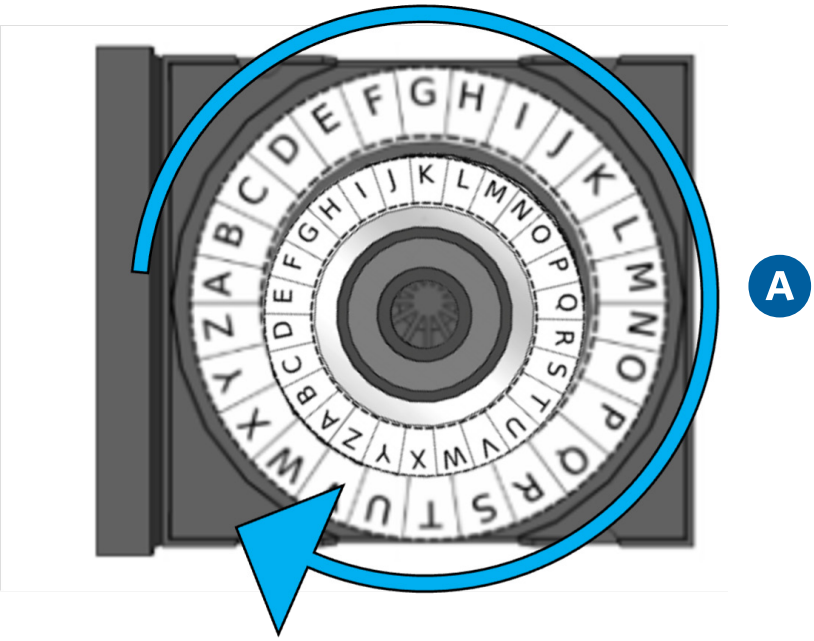
For example, 29 mod 26 = 3



NAME _____ DATE _____

When y - k mod 26 is less than 0, the letters are determined in the same way, except the disc codes counter-clockwise.

For example, -4 mod 26 =22



The Caesar Cipher allows quick and easy translation of coded messages. Computer algorithms, similar to the Caesar Cipher, are used to secure modern-day internet transactions. One problem, however, is that these security systems may be easily de-coded by computers and robots.

Luis von Ahn developed a way to protect against these types of threats called CAPTCHA and re-CAPTCHA. Both methods rely on visual "codes" that only humans can read and enter into a computer to access secure websites.

Acknowledgment: Permission granted by the Resource Area for Teachers