raft resource area for teaching
www.raft.net

**Curriculum topics:**

- Ancient civilizations
- Cryptography
- Functions
- Modular arithmetic
- Patterns

**Subject:**
**Mathematics, Social Studies**

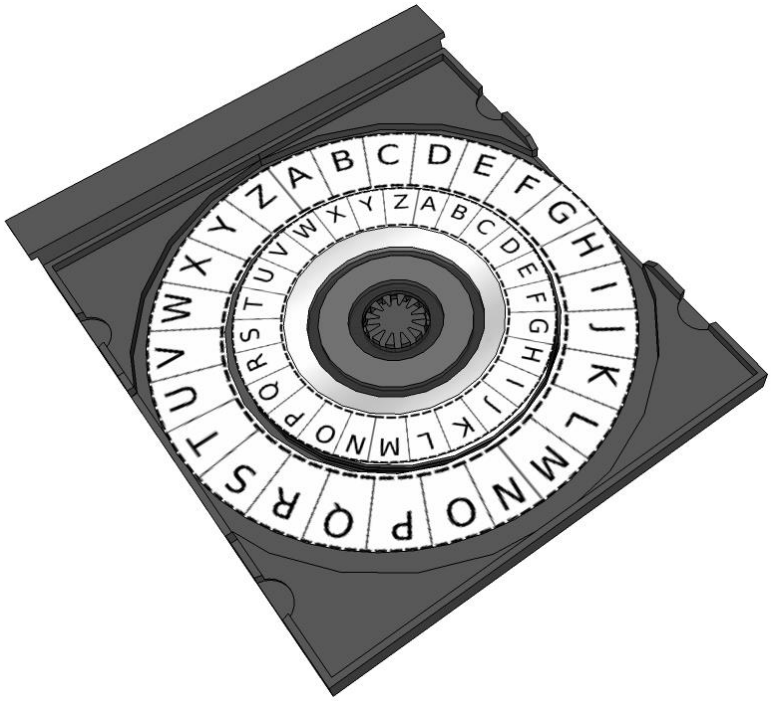
**Grade range: 3 – 12**

# CAESAR CIPHER DISC

Learn cryptography the Roman way!



Cryptography was important more than 4,000 years ago as a way to protect the interests of kings, military leaders, and other dignitaries. It is important today because of the vast amounts of personal, financial, and medical data stored in computer systems worldwide. Students will appreciate cryptography in terms of math and history by encoding and decoding messages using a technique similar to that used by the Roman general Julius Caesar!



**Who we are:**

Resource Area for Teaching (RAFT) helps educators transform the learning experience through affordable "hands-on" activities that engage students and inspire the joy and discovery of learning.

**For more ideas and to see RAFT Locations**

www.raft.net/visit-raft-locations



http://www.raft.net/raft-idea?isid=730

# Materials required

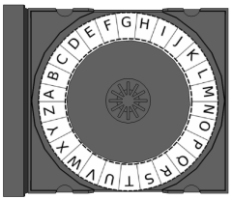
Per cipher disc:

- Mini CD, ~7.5 cm (3 inch) or equivalent-sized circle
- Media tray for standard CD
- Black line master for Caesar Cipher disc pattern (templates can be downloaded at http://www.raft.net/raft-idea?isid=730)
- Tape or glue
- Scissors

# How to build it

**1** Cut out the ring templates from the black line master sheet.

**2** Tape or glue large template onto media tray (A) and small template onto mini CD or equivalent circle (B).

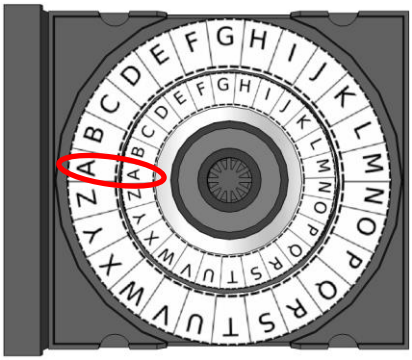


A

B

**3** Place mini CD or circle into media tray.

**4** Align the A's on the templates (circled below).



# Learning to use the cipher disc:

1. The small ring contains the plaintext letters to be encoded. The large ring contains the cipher text (encoded plaintext letters).

2. Encoding HELLO with key of 3: Turn the mini CD 3 positions to the right (clockwise). The first plaintext letter in HELLO is H. The cipher text letter on the outer ring is K.

3. Continue encoding the rest of the word HELLO. When finished, the plaintext word HELLO becomes the cipher text word KHOOR.

*Encode: Shift the letters according to the key. Read from inner ring to outer ring*
*Decode: Shift the letters according to the key. Read from outer ring to inner ring*

# To do and notice

1. Realign the A's. Decode the following notable cipher text messages using the keys given. (Answers are at the bottom of the page.)

   "F UJSSD XFAJI NX F UJSSD JFWSJI" – Benjamin Franklin, **[key: 5]**

   "LKB PJXII PQBM CLO JXK, LKB DFXKQ IBXM CLO JXKHFKA" – Neil Armstrong, **[key: −3]** (For keys that are negative, rotate the mini CD counter-clockwise).

   "NWPLC PJPD QFWW SPLCED NLY'E WZDP" – Eric Taylor ("Friday Night Lights"), **[key: 11]**

2. Choose a whole number (positive or negative) to serve as a secret key. Create your own encoded message and let others try to decode the message

# The content behind the activity

Cryptography is the practice of techniques for secure communication including data integrity, authentication, and confidentiality.

**History**
Julius Caesar, a famous general of the Roman Republic who later became its first emperor, protected important messages using this encryption scheme, which takes an original message and converts it to an encoded message. The cipher encodes messages by substituting letters with other letters further away in the alphabet. For example, the message "SURPRISE" might become "VXUSULVH".

**Math**
The Caesar cipher is a substitution cipher where the encryption function uses modular arithmetic to shift the letters. Formally, the encryption and decryption functions can be written as:

$$E(x, k) = (x + k) \bmod 26 \qquad D(y, k) = (y - k) \bmod 26$$

E is the encryption function, D is the decryption function, x is the plaintext letter, y is the cipher text letter, and k is the secret key. Arithmetic is done as normal except when x + k is greater than 26. In this case one determines the cipher text by reading the disc all the way around in the clockwise direction, returning to the starting letter position and continuing to the indicated position (e.g. 28 mod 26 = 2). When y - k mod 26 is less than 0, the plain text is determined the same as above except the disc is read counter-clockwise (e.g. -3 mod 26 = 23). The Caesar cipher is simplistic and easily broken. Modular arithmetic, however, continues to secure virtually all Internet transactions using sophisticated and secure encryption schemes involving exponentiation, prime numbers, and integer factorization.

- A Penny Saved is a Penny Earned
- One Small Step for Man, One Giant Leap for Mankind
- Clear Eyes Full Hearts Can't Lose

Curriculum Standards:

Identifying arithmetic patterns (Common Core Math Standards: Grade 3, Operations & Algebraic Thinking, 9)

Use rules to generate number patterns (Common Core Math Standards: Operations & Algebraic Thinking, Grade 4, 5; Grade 5, 3)

Writing and evaluating single-variable expressions (Common Core Math Standards: Grade 6, Expressions & Equations, 2)

Defining, evaluating, & comparing functions (Common Core Math Standards: Grade 8, Functions, 1-3)

Problem Solving and Reasoning (Common Core Math Standards: Mathematical Practices, Grades 3-12)

Science has a major influence on social and cultural change (Science, Technology, and Society)

# Learn more

- Develop a "lost key" protocol by creating clues one might follow in order to figure out the key with which to decode the message. For example, a clue might be a single-variable equation that when solved for reveals the key.
- Create messages with unknown encryption keys for peers to solve.
- Write out the encryption and decryption functions for different message.
- Convert encrypted messages into binary code
- Try to encrypt a message using the alphabet from a foreign language
- Change key values at specific points in message, making it harder to decode
- Create an equation with 2 or more solutions to find a key: one could be the true key while the other is false. Alternatively, the keys could change partway through the message.

**Related activities:** See RAFT Idea Sheets:

**Messages & Codes:**

***Binary Birthday Bracelets -***
http://www.raft.net/ideas/Binary Birthday Bracelets.pdf

***Break the Code -***
http://www.raft.net/ideas/Break the Code.pdf

**Functions:**

***Dive into Square Pools -***
http://www.raft.net/ideas/Dive into Square Pools.pdf

***Shape Up with Algebra –***
http://www.raft.net/ideas/Shape Up with Algebra.pdf

# Resources

Visit www.raft.net/raft-idea?isid=730 for "how-to" video demos & more ideas!

See these websites for more information on the following topics:

- **Cryptography overview** – http://www.garykessler.net/library/crypto.html
- **Cryptography techniques** – http://www.cerias.purdue.edu/education/k-12/teaching_resources/lessons_presentations/cryptology.html

## Acknowledgements:

Based on a classroom activity developed by Kaisen Lin.