# CODES, CIPHERS, AND SECRETS

Anne M. Ho
CCU Math Teachers' Circle
Spring 2017

**Cryptography** is the study and practice of secure communication. Cryptography uses mathematics, computer science, and engineering. Computer passwords, bank account information, online shopping, ATM cards, emails, etc. all use cryptography.

## Brainteaser

Teachers are presented with a padlock and are given clues to unlock them.

- 9761: This lock shows different ways we can use padlocks with math problems. We can use computations or definitions.

> The positive solution to $x^2 + 2x - 99 = 0$.
> The $y$-coordinate corresponding to $x = 3$ for the line $y = x + 4$.
> The multiplicity of the zero 3 in the equation $3x(x-3)^6(x+3)^5 = 0$.
> Given $f(x) = e^x$. What is $f(0)$?

- 2020:

> The next year in which we'll have a leap year.

- 1009:

> The smallest 4-digit prime number.

- 8157: Trial and error will open the lock. There are 10 possibilities for the last digit.

> The code is `815X`.

- 4231: Note that there are $4! = 24$ possibilities. Trial and error will open the lock.

> Some permutation of the digits 1, 2, 3, and 4.

## 1. Shift (Caesar) Ciphers

1.1. **Translating Letters Into Numbers.** First of all, we can create a correspondence between letters and numbers as follows:

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Example 1.** What does the word "`dog`" translate into?

**Example 2.** What does the word "`mathematics`" translate into?

**Example 3.** What does your first name translate into?

1.2. **Encryption.** To encrypt a secret message, we use a **cipher**. A classic cipher is the **shift (or Caesar) cipher** (said to be used by Julius Caesar).

> In cryptography, the message that is being encrypted is called the **plaintext**. The encrypted message is called the **ciphertext**.

**Example 4.** The letter `a` corresponds to the number 0. If we shift it by 3 spaces down the alphabet, we get 3, which corresponds to the letter `d`. If we shift `z` down by 3 spaces, we start over at the beginning of the alphabet and end up with `c`.

**Example 5.** Shift the digits for the word "`dog`" by 3 spaces down the alphabet.

**Example 6.** Shift the digits for your first name by 5 spaces down the alphabet.

1.3. **Functions and Modular Arithmetic.** We can think of ciphers as **encryption functions**. The input is the set of digits for the plaintext, and the output is the set of digits for the ciphertext. We just have to remember to use **modular arithmetic**.

**Modular arithmetic** is like "clock arithmetic."

- 13 o'clock is the same as 1 o'clock. Notation:

$$13 \bmod 12 \equiv 1 \bmod 12.$$

- 28 o'clock is the same as 2 o'clock. Notation:

$$28 \bmod 12 \equiv 4 \bmod 12.$$

- In general, we write $a \bmod n \equiv b \bmod n$ for nonnegative integers $a, b$, and $n$ if $a - b$ is a multiple of $n$.
- Fill in the blanks for the following (there is more than one unique answer!):

1. _____ $\equiv 3 \bmod 4$
2. _____ $\equiv 7 \bmod 9$
3. _____ $\equiv 11 \bmod 13$
4. _____ $\equiv 0 \bmod 26$
5. _____ $\equiv 2 \bmod 26$
6. _____ $\equiv 11 \bmod 26$
7. _____ $\equiv -1 \bmod 26$
8. _____ $\equiv -4 \bmod 26$

1.4. **Encryption and Functions.**

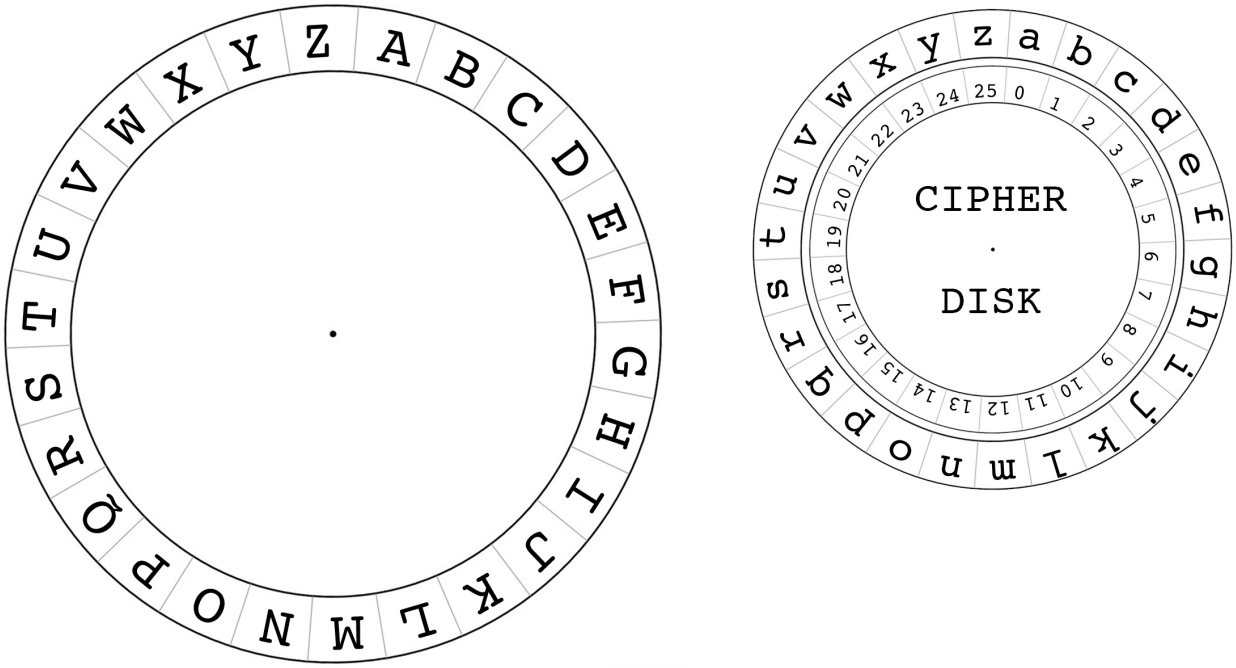
**Example 7.** For the shift by 3 function, we can write

$$f(x) \equiv x + 3 \bmod 26.$$

**Example 8.** If the plaintext of a message has the letter "a" corresponding to the ciphertext letter of "x," what is the encryption function?

**Example 9.** If the plaintext of a message has the letter "e" corresponding to the ciphertext letter of "c," what is the encryption function?

These cipher disks may help with this process. These can be printed, cut out, and pieced together with a brad.




1.5. **Decryption.** So far, we have **encrypted** information, but we also want to **decrypt** information.

**Example 10.** Write a one-word (secret) message, and encrypt it using the function

$$f(x) \equiv x + 4 \bmod 26.$$

We will exchange papers with someone in the room. Once you receive a friend's ciphertext, what is your strategy for decrypting (i.e. finding the original plaintext)?

1.6. **Inverse Functions.** We can think of decrypting as using the **inverse function**, or the function that "reverses" the encryption function.

**Example 11.** If $f(x) \equiv x + 3 \bmod 26$ is the encryption function, then $g(y) \equiv y - 3 \bmod 26 \equiv y + 23 \bmod 26$ is the decryption function.

**Example 12.** If $f(x) \equiv x + 8 \bmod 26$ is the encryption function, what is the inverse function or decryption function?

How is this related to how we teach inverse functions? How is it different?

## 2. Affine Ciphers and Linear Functions

Notice that our encryption and decryption functions are **linear functions** with a slope of $m = 1$. We can also have encryption and decryption functions with other slopes. These are **affine ciphers**, and their encryption function looks like $f(x) \equiv mx + b \bmod 26$ for some positive integers $m$ and $b$.

**Example 13.** Use the affine cipher $f(x) \equiv 3x + 7 \bmod 26$ to encrypt the plaintext letter "c." What is the corresponding ciphertext? What about for "d?"

What would be challenging about finding decryption functions for affine ciphers?

It turns out that finding inverses is particularly difficult because not all numbers have inverses modulo 26. Here is a table of all possible inverses in the mod 26 system:

| Number | Inverse |
|---|---|
| 1 | 1 |
| 3 | 9 |
| 5 | 21 |
| 7 | 15 |
| 9 | 3 |
| 11 | 19 |
| 15 | 7 |
| 17 | 23 |
| 19 | 11 |
| 21 | 5 |
| 23 | 17 |
| 25 | 25 |

## 3. Recommended 5-Day Lesson Plan

1. General Introduction to Cryptography: What is it? Where has it been used? Why is it important?
2. Modular Arithmetic and Caesar Cipher
3. Functions and Encryption Using Shift Ciphers
4. Inverse Functions and Decryption
5. Equation of a Line and Affine Ciphers

## 4. Resources


- Beck, Matthias (2008). "The Teacher's Circle: Codes, Ciphers & Secret Messages." *Math Teachers' Circle*. `http://www.mathteacherscircle.org/assets/session-materials/beck.codes.pdf`.
- Davis, Tom (2013). "Information, Compression and Cryptography." *Math Teachers' Circle*. `http://www.geometer.org/mathcircles/crypto.pdf`.
- Singh, Simon (1999). The Code Book. Anchor Books.


**Instructions for Setting Lock**

The original number is 0000. To set your own combination, follow the steps:

1. Pull up the shackle to open the lock.
2. Rotate the shackle 90 degrees counterclockwise and press all the way down. Hold down.
3. Set your own combination by turning dials.
4. Turn the shackle back as normal. Then the setting is complete.