# Make a Caesar Cypher

## Key concepts

* Patterns
* Code
* Puzzles
* Cryptography

## Introduction

If you need to send a secret message to a friend, how could you prevent other people from reading it? One way is to encrypt the message—that is, use a secret code that only you and your friend know. Try this activity to learn how to create your own “Caesar cipher,” a popular type of code that is easy to learn.

## Background

Cryptography is the study of writing or solving secret codes that are used for secure communication. Historically, codes have been used by politicians, spies and countries at war to prevent their enemies from knowing what they’re up to. Many of the earliest codes, or “ciphers,” such as the one you will create in this project were easy to create by hand. Now cryptography is essential in computer science for keeping everything from e-mails to bank account information secure.

The Caesar cipher, named after Roman Emperor Julius Caesar is one of the earliest and most widely known ciphers. It is a simple form of a “substitution cipher” where you replace each letter of the alphabet with another letter by shifting the whole alphabet a certain number of letters (wrapping around to the beginning once you reach the end). For example, this would be your key and code if you shift each letter by three spaces:

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ  
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

So, when you write your message, the letter A gets replaced with X, B gets replaced with Y and so on. For example, the word “HELLO” reads:

Plain: HELLO  
Cipher: EBIIL

In order to decode your message, you need to share the “key” (the number 3) with your friend. After that you can send messages that are written in cipher so other people can't read them!

## Materials

Pencil and paper

At least one other person

## Preparation

Explain the concept of a Caesar cipher to a friend or have them read the background section of this activity.

Write down the alphabet from A to Z.

Pick a number from 1 to 25. (If you use 26, you will just wind up with the original alphabet.) This number is your key.

## Procedure

Shift the entire alphabet by the number you picked and write it down below your original alphabet (as shown above).

Pick a message to write to your friend. It might be easiest to start out with a simple message (such as a single word or phrase) before you try longer sentences or paragraphs.

Write down your encoded message using your shifted alphabet. If it helps, write down your plain text message first then encode it one letter at a time (such as the “hello” example above). Just make sure the piece of paper you give your friend only has the encoded message!

Give your friend the encoded message and tell them the key. Why do you think you wouldn't want to write down the key?

See if your friend can decrypt your message. If it helps for the first try, let them work backward using the original and shifted alphabets you wrote down. Using the example from the background, the letter x becomes a; y becomes b; and so on.

Try switching and using a different key for the same messages. Do either look easier to crack?

Extra: Try finding a third person who does not know what a Caesar cipher is. Can they crack your code if they “intercept” your message?

Extra: What if the person who intercepts your message knows about Caesar ciphers? Does that make it easier to crack the code? Because there are only 25 possible keys, Caesar ciphers are very vulnerable to a “brute force” attack, where the decoder simply tries each possible combination of letters. This might take some patience if a human does it, but nowadays computers can unravel the code in a fraction of a second, so Caesar ciphers are not considered a secure method to encrypt electronic communications.

Extra: Another way to crack the Caesar cipher is “frequency analysis,” which is based on the fact that in natural English speech and writing, certain letters appear much more frequently than others. For example, the letter E appears more often than any other one whereas Z appears the least often. (If you have ever played the board game Scrabble, you might notice that this determines how many points letters are worth!) So, for example, if you read an entire paragraph and notice that the letter D appears more often than any other, odds are that it used a Caesar cipher with a shift of 1 (making E a D in the code). This technique will be more accurate for longer blocks of text and very inaccurate for short words or phrases because there are plenty of words that do not contain E at all. Can you have a friend write an entire paragraph with a Caesar cipher and then try to crack it using frequency analysis?

Extra: If you plan to use the Caesar cipher for regular communication, one risk is that eventually someone will discover your key. You can help prevent this by changing the key, for example using a new one every week. This is a similar concept to periodically changing your computer passwords.

Extra: The Caesar cipher is just one type of substitution cipher. Look up some other types of substitution ciphers and try them out. Are they harder or easier to use and crack?

## Observations and results

Once you and your friend both understand how to use a Caesar cipher it should be relatively easy to send encrypted communications to each other. This can be a fun way to pass secret messages back and forth between friends. As discussed above, however, although the Caesar cipher provides a great introduction to cryptography, in the computer age it is no longer a secure way to send encrypted communications electronically.