**Cryptography**



**The Caesar Cipher:**

The Caesar Cipher gets its name from Julius Caesar, the Emperor of Rome in ancient times. Caesar would send secret messages to his troops using this method. Let’s learn this method of encoding secret messages. We all know that there are 26 letters in the alphabet. If we consider

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A=0 | B=1 | C=2 | D=3 | E=4 | F=5 | G=6 | H=7 | I=8 | J=9 | K=10 | L=11 | M=12 |
| N=13 | O=14 | P=15 | Q=16 | R=17 | S=18 | T=19 | U=20 | V=21 | W=22 | X=23 | Y=24 | Z=25 |

We get a natural numbering of the alphabet. The Caesar Cipher works by shifting the letters either forward or backward (called the key).

Let’s consider the word ZOMBIE.

This word becomes the numerical sequence \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Consider the numerical sequence 18 13 0 8 11.

This sequence corresponds to the word \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

To encode the word ZOMBIE using a key(shift) of 5, we will add 5 to each number in the numerical sequence you found earlier.

Adding 5 gives the numerical sequence for ZOMBIE gives 30 19 17 6 13 9

Notice that we arrived at some numbers larger than 25 in our numerical sequence. To adjust for this we perform modular arithmetic.

**Modular Arithmetic:**

The use of modular arithmetic is more common than you think. Consider military time of 22 hundred hours. Since 22 is larger than 12, this time is referring to a pm time. To get at the time we can subtract 12 from 22, giving 10. Thus 22 hundred hours military time is equivalent to 10:00 pm. We may also arrive at 10, by observing when we divide 22 by 12 we get a remainder of 10. Mathematicians write 10 ≡ 22mod(12).

Dividing 30 by 26, we get a remainder of \_\_\_\_\_\_\_\_\_\_\_\_.

Thus our shifted sequence is 4 19 17 6 13 9. Giving the coded word \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Try coding the message MEET ME AT NOON using a key of 14 in the space provided below:

**Decoding the Caesar Cipher:**

The Caesar Cipher is a breakable code. In other words, with enough analysis you can determine the keys for a Caesar Cipher. We will focus on a technique called frequency analysis. Frequency analysis refers to the fact that certain letters seem to appear more common in the English language than others. Below is a chart of frequencies of letters in the alphabet:



So we see that the letter “e” seems to show up the most, followed by “t”, “a”, and so on. Using these frequencies, we can make educated guesses at what the shift (key) is.

The following coded message was found directly outside the sushi restaurant:

NOKN YX IYEB POOD? TYSX EC PYB K DBOKD!

To decode this message using frequency analysis we first need to count the number of times each letter appears in the message. This is called the letter's frequency.

Here we see that B has frequency 3 since it appears 3 times in the code. Count the number of times each letter appears and record its frequency below:

B = \_\_\_\_\_\_\_\_\_ C = \_\_\_\_\_\_\_\_\_ D = \_\_\_\_\_\_\_\_\_ E = \_\_\_\_\_\_\_\_\_ I = \_\_\_\_\_\_\_\_\_

K = \_\_\_\_\_\_\_\_\_ N = \_\_\_\_\_\_\_\_\_ O = \_\_\_\_\_\_\_\_\_ P = \_\_\_\_\_\_\_\_\_ S = \_\_\_\_\_\_\_\_\_

T = \_\_\_\_\_\_\_\_\_ X = \_\_\_\_\_\_\_\_\_ Y = \_\_\_\_\_\_\_\_\_

Notice that O and Y appear the most in the code. Since “e” has the highest frequency, it is a good guess that the letter E was coded to the letter O or Y. So we have to make a guess, if our guess is incorrect that is OK! If E = 4 was coded to O = 14 that would imply a shift of +10. So to decode we will shift it back with a shift of -10. Let’s try out that shift on our first word in the code NOKN. NOKN numerical sequence is 13 14 10 13, subtracting 10 from each number in the sequence we get 3 4 0 3. The sequence 3 4 0 3 corresponds to the word DEAD. Notice that this is a word in the dictionary, so our guess of a shift of 10 seems to be correct!! Decode the rest of the message in the space provided below. Don’t forget to use modular arithmetic when needed:

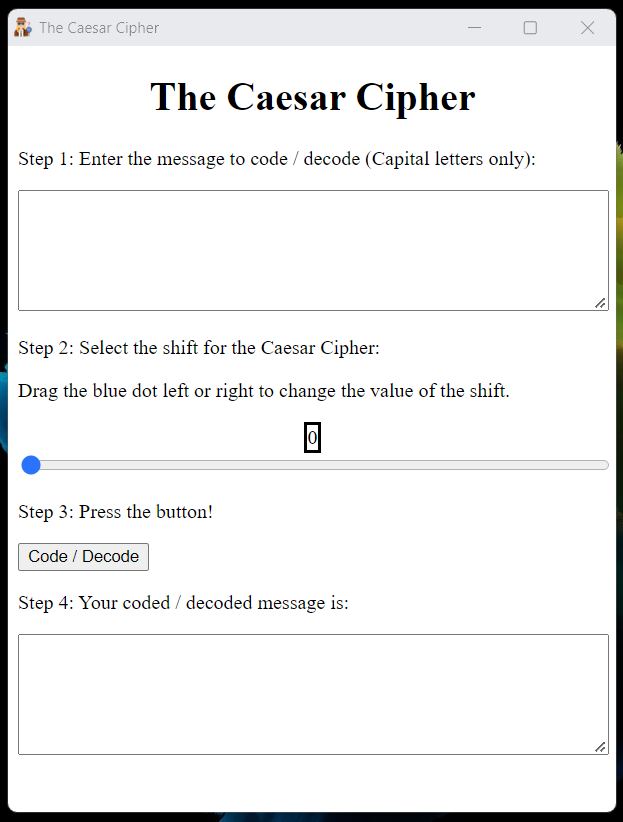
**Using a Program to Code a Message:**

Writing a computer program can let us do some things, like coding or decoding a message with the Caesar Cipher, much more quickly than if we did it by hand.

To see this in action, first double click the Caesar Cipher icon on your computer. It looks like this:



You should see this on your screen:



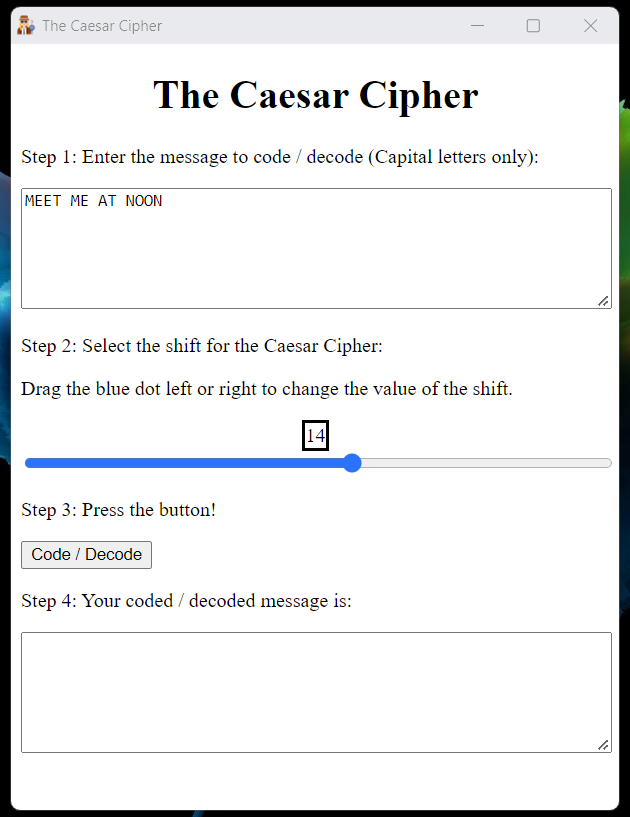
Click inside the white box under **STEP 1** and type MEET ME AT NOON in the box.

Next, go to **STEP 2**. We are going to pick the shift to use for the Caesar Cipher. Use the left mouse button to press on the blue dot on the slider bar. While pressing the button drag the blue dot left or right to change the value in the box above the slider bar until the number is 14. The screen should look like this:

**Enter your message here**

**Change the shift here**

**The coded / decoded message will show up here**



When you're ready, click the **Code / Decode** button. Look in the box under **STEP 4** and write down the message in the space below. Does the message match what you did by hand before?

Now try coding these messages using the program.

The message CRYPTOGRAPHY IS FUNwith a shift of 5 becomes

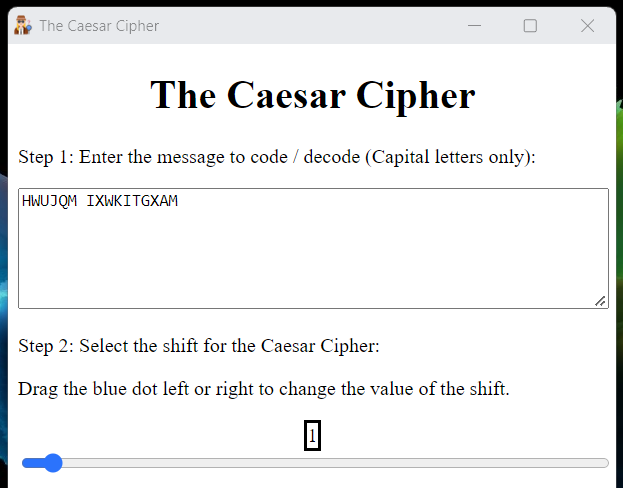
The message GIRLS IN SCIENCE with a shift of 19 becomes

**Using a Program to Decode a Message:**

We can also use the program to decode a message, even if we don't know what the shift is. Enter

HWUJQM IXWKITGXAM

in the box for **STEP 1**. Under **STEP 2**, move the blue dot to display the number 1. The top part of your screen should look like this:



Now press the **Code / Decode** button and look in the box under **STEP 4** for the decoded message. Does this message make sense? If it doesn't, then we guessed the wrong shift.

Try different numbers for the shift until you get a message that makes sense. When you find the message, fill in the blanks below.

HWUJQM IXWKITGXAM uses a shift of and decodes to

What other coded messages have you seen today? Use the space below to keep track of these messages and try to decode them.