# Homework 1

August 24, 2020

## 1 Caesar Ciphers Explained

Caesar Ciphers work on the idea that two people Alice and Bob want to send data to each other and they want to hide their message by shifting the letters over to the right by a secret amount only known by Alice and Bob. It is one of the earliest encryption systems, developed in Ancient Rome and named for Julius Caesar, who used it for encoding military messages.

True to the original tradition, We will be working with a fixed alphabet `ABCDEFGHIJKLMNOPQRSTUVWXYZ`. To keep things simple, all letters will be capitalized and we will not be encoding any other symbols. For example, a right shift of five positions in our alphabet would look like this `GHIJKLMNOPQRSTUVWXYZABCDEF`.

Notice how all of the letters are shifted over by five positions. So as an example of how you can use the shifted alphabet to encode a word "HELLO" you translate the letter by looking up its normal position in the shifted alphabet. Since `H` is the 8th letter (7 if you start from 0) you would output the 8'th letter in the shifted alphabet, which is the letter `M`. The process is repeated for each subsequent letter. `E` (the 5th letter) is translated as `M`, `L` as `Q`, etc.

The receiver would receive the message `MJQQT`.

To decode the message, you do the reverse and look at the key (6) and perform the reverse encoding to get HELLO.

While this cipher might be straightforward, it remains one of the interesting ones from a historical point of view and was even used to build many variations that are hard to crack.

## 2 Assignment

Your job is to decode a text file where every **sentence** has a different Caesar Cipher shift.

You will have to read from `stdin` (standard input) dynamically, split the input line into words, and then figure out the Caesar cipher encryption for that specific sentence.

There are **26 possibilities** for each sentence.

Below is a decoding algorithm written with Python syntax (chosen because many students may have seen it and it is easy to read) that decodes a word.

We will give you a file of all possible words that appear within the stream. Your job is to find the specific Caesar Cipher shift for each sentence from the input. Once you reach the end of stdin, the program should close and there should be a file where each line number of the file represents the sentence.

Once the sentence is saved you have to iterate through it by word, shift the word until it matches a word in the dictionary. Once all of the words in the sentence match, with a singular shift we save the sentence number and the shift amount in a file.

```
Write your sentence shift to a file called shifts.txt
The output will look like this:

#Below is the first line in the file
1 #What this tells me is the first sentence has a Caesar shift of 1
```

```
2 #sentence two had a Caesar shift of 2
5 #sentence three had a Caesar shift of 5
.
.
. Processes n sentences
.
.
14 #sentence n had a Caesar shift of 14.
```

## 3 Grading

You will be graded using the following criteria.

1. Able to parse a sentence from stdin 1 point
2. Code is readable and commented 1 point
3. GitHub is used properly 1 point
4. Code is able to write results to a file 2 points
5. Code is able to correctly determine the Caesar cipher of each sentence 5 points

## 4 Enrichment and Challenge Opportunities

While we don't necessarily award extra credit in this class, there are opportunities to distinguish yourself. Here are some possibilities.

1. Allow for upper and lowercase input, but use the uppercase translation table to handle both. Use case-insensitive comparison to identify words when determining whether you have "cracked the key" so to speak.
2. Allow for symbols not in the alphabet by gently ignoring them. Since a word is defined as being anything in the alphabet, assume anything not in the alphabet was not encoded (or to be decoded). This would allow punctuated text to pass through during processing.
3. Have an option to write the decoded text to a line, with its shift value (e.g. shift value:decoded text) to the standard output. Write a second program that takes the colon-separated shift:decoded-text and recreates the encoded text file.