On Caesar Ciphers

A Caesar cipher is a simple cryptography technique where letters of the alphabet are shifted by a fixed amount, and plaintext is replaced by characters which are shifted. For example, ROT13 is the most-known case of Caesar ciphers, and refers to its rotation by 13 spots. Because there are 26 letters in the Latin alphabet, ROT13 can encrypt and decrypt using the same algorithm, unlike other rotations.

For example, say we have the word “MEOW”. By ROT13, we could find that our characters would shift according to the following plan:

```
Original: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
New:      N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
```

So, by taking each letter and checking which letter matches up to it in the “New” list of letters, MEOW would become ZRBJ. If you try to work backwards by entering ZRBJ into the above key where ZRBJ are the original letters, you will also end up back at MEOW!

Field guide for solving wild Caesar Ciphers

Say you come across a wild Caesar cipher to decode in life, such as the one which is in the game you’re playing. How can you approach it?

In general, it will likely be easiest to write out the new alphabet in its entirety, doing exactly what we did for the ROT13 example, so that you can easily translate from the original text to something new. Once the shifted alphabet is spelled out, you will just need to go character-by-character and map everything out to the new alphabet.

Since there are 26 letters in the alphabet, you could only form at most 25 different shifts, so your most simple brute force algorithm would be trying all of these rotations and seeing if your result seems at all coherent. In addition, you might be able to save yourself some time by guessing. For example, maybe you are given a phrase in the following form:

vhlch wkh gdb

You could start solving this by working through rotations one-by-one, starting with ROT1 and ending at ROT25. But, is it possible to try specific rotations instead and get to the end result a little bit faster? We can see that there is a three-letter word in the middle of the phrase. What three-letter words in the middle of phrases are most common? You can first try making guesses based on your guess of what the original word might be, so here, we’re going to try finding the rotation that would make “wkh” map out to a very common word, “the.”

So, we can start with the first character, w, and shift the entire alphabet so that a “t” in the original alphabet would map to a “w” in the new alphabet. Now that we have this shifted alphabet, we could see where the other characters fall.

```
Original: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
New:      D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

So, the other two characters to check in “the” are the “h” and “e.” If we look at “h” in the original alphabet, we see it maps out to “k”, which is promising. It would seem that “wk” is mapping to “th”, so we just need to see if “wkh” really does become “the” by checking “e” in the original alphabet. The “e” DOES appear to map to “h” in the new alphabet, so since we’re pretty confident “the” is a real word, we can try translating the rest of the phrase! This would mean ‘3’ is a possible rotation number.

Current progress on decrypting: ----- the ---

If we continue with our decryption using 3 as the rotation number, we discover that the phrase translates to “seize the day”! Note that, for the rest of the phrase, it might be easier to start from the new alphabet and work backwards, rather than do what we did for guessing “the”. So, to translate “vhlch” into “seize”, we find “v” in the new alphabet, and look up at the original. In the original alphabet, we can see that “s” lines up with the “v” in the new alphabet, and go from here with the rest of the word.

Other than trying to guess a common word such as “the”, you could try thinking about common word structures. Words tend to have vowels early on in them, eg. either the first or second letter will probably be an “a”, or “e”, or “i”, or “o”, and so on. So, you could try lining up an encrypted cipher with these guesses in mind in hopes of making the translation efforts a bit faster.

If all of these techniques fail, then there are still ways that you can decrypt/encrypt Caesar ciphers. Look them up on your search engine of choice, and you’re likely to find some tools that can help!