Caesar Cipher

*Encrypting and decrypting code*

Julius Caesar, in his campaigns to conquer the world, encrypted his messages using a simple technique now named after him; he simply wrote the message with the letters shifted over by a certain number of positions. In other words, if all the letters were to be regarded as shifted over by one, all As in the message would be Bs and Bs would be written C, etc.

Write a program to encrypt messages by the Caesar method. Allow the user to enter the Caesar shift required. In other words, if the user decides to use a Caesar shift of 3, all As become Ds, etc.

Have a second part that will accept the encrypted message and the Caesar shift, and unravel the message again.

*Decryption without the key.*

If you do not know the Caesar shift, but you have the ciphertext, you can still unravel the message quite easily. In English, certain letters have a greater frequency than others, so if all Os were encoded as Xs, you can work out which letter the X stands for by frequency analysis. Below is a table of the letter frequency for English:

|  |  |  |  |
| --- | --- | --- | --- |
| A | 8.2% | N | 6.7% |
| B | 1.5% | O | 7.5% |
| C | 2.8% | P | 1.9% |
| D | 4.3% | Q | 0.1% |
| E | 12.7% | R | 6.0% |
| F | 2.2% | S | 6.3% |
| G | 2.0% | T | 9.1% |
| H | 6.1% | U | 2.8% |
| I | 7.0% | V | 1.0% |
| J | 0.2% | W | 2.4% |
| K | 0.8% | X | 0.2% |
| L | 4.0% | Y | 2.0% |
| M | 2.4% | Z | 0.1% |

Write a program that will work as follows:

* Allow the user to type in the encrypted code.
* Count the occurrences of letters of the cipher text and give a percentage of the occurrence of each.
* Let the user use his brain to compare cipher text frequencies to the plain text frequencies. The user can exchange letters in the message as follows:
* The user enters a cipher text letter from the message he’d like to decipher, then enters the letter he’d like to replace it with. The program then replaces all the occurrences of the cipher text letter with the plaintext letter.

The user continues this way, replacing letters by detective work and guesswork, until the message is decoded.

To make it easier to tell the cipher text letters from the plaintext letters, use this convention: cipher text letters are all uppercase, and plaintext letters are all lowercase.

*Source: Singh, S, 1999. The Code Book. London*