Caesar Cipher technology

Caesar cipher is s a type of encryption based on substitution cipher. Substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet.

For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

The method is named after Julius Caesar, who apparently used it to communicate with his generals.

Mathematical Description

First, let's assign numbers to all characters. e.g., $'a' = 0, 'b' = 1, 'c' = 2, \ldots, 'z' = 25$.

We can now represent the Caesar cipher encryption function, $e(x)$, where x is the character as an input:

$$e(x) = (x + k) \pmod{26}$$

And k is the key (the shift) applied to each letter.

After applying this function the result is a number which must then be translated back into a letter.

The decryption function is:

$$e(x) = (x - k) \pmod{26}$$

Now your turn

2 Use the Caesar cipher to encrypt and decrypt the message "HELLO," and the key (shift) value of this message is 14.

Hint: use either the mathematical formula or encrypt it manually by shifting each letter as required.

What about if the shift number is negative, rewrite the formula?

2 Use the Caesar cipher to encrypt and decrypt the message "HELLO," and the key (shift) value of this message is -14