Caesar-Cipher

Piyush Mohanty

History

1. The Caesar cipher is a type of substitution cipher named after Julius Caesar.
2. It involves shifting each letter of the alphabet by a fixed number of positions down the alphabet.
3. Julius Caesar used a shift of three to protect military messages, and Augustus used a shift of one.
4. More complicated systems were also used by Caesar, and evidence of this exists in historical records.
5. It is unknown how effective the Caesar cipher was at the time, as there is no record of techniques for solving simple substitution ciphers.
6. The cipher is still used today in children's toys and the ROT13 algorithm.
7. The Vigenère cipher uses a Caesar cipher with a different shift at each position in the text.
8. The one-time pad cipher is a variation of the Vigenère cipher and is proven unbreakable under certain conditions, although these conditions are very difficult to achieve.
9. The Caesar cipher has been used in personal advertisements and even by the Russian army in World War I.
10. Fugitive Mafia boss Bernardo Provenzano was captured in part because of his clumsy use of a variation of the Caesar cipher.
11. Rajib Karim was convicted of "terrorism offences" in the UK in 2011 for using the Caesar cipher to communicate with Bangladeshi Islamic activists.

Caesar Cipher Algorithm

Letters are replaced by other letters or symbols

It is a type of shift cipher and the earliest one to be used by Julius Caesar.

Usually, 3 is used as the key for Caesar Cipher i.e. (shift cipher with key 3 is called Caesar Cipher).

C = E(p, k) mod 26 = (p+k) mod 26

P = D(c, k) mod 26 = (p-k) mod 26

Where ‘P’ is plain text, ‘C’ is cipher text, ‘E’ is the encryption algorithm, ‘D’ is the decryption algorithm, and ‘k’ is the key.

(Here, "mod" refers to the modulo operation. The value *x* is in the range 0 to 25, but if *x* + *n* or *x* − *n* are not in this range then 26 should be added or subtracted.)

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Deciphering is done in reverse, with a right shift of 3.

Advantages

Easy to memorize and implement.

Key values are within 25.

Disadvantages

The Caesar cipher can be easily broken using brute force techniques or frequency analysis due to its limited number of possible shifts. The distribution of letters in English language text can also help determine the shift. The unicity distance for the Caesar cipher is about 2, meaning at least two characters of ciphertext are required to determine the key. Encrypting a text multiple times using different shifts provides no additional security as it is equivalent to a single encryption with a combined shift.