

Caesar Cipher

The Caesar cipher is a simple cipher and one of the best known encryption algorithms. It is very simple to encrypt, decrypt and intercept. The Caesar cipher is a substitution cipher where each letter in the plain-text (decoded text) is replaced by a letter a certain number of spaces to the right of the letter in the alphabet. (The amount of spaces is called the key or shift and is only known by the sender and intended receiver).

Disclaimer: Do not attempt to encrypt personal data or serious messages with this cipher!!! It takes only half a second to crack by a computer!

1. It takes a very small amount of time to encode and decode messages. (Less than a second, usually)
2. No real applications exist for the cipher as it is the most insecure out there.
3. This cipher was invented by Julius Caesar as a way to send messages of high military significance.

Steps

Encryption

1. Choose the alphabet you are going to use.
2. Choose a secret key (shift) that you are going to use in this case **n**.
3. For every letter in the plain-text, replace it by a letter of the alphabet that is **n** letters away from the letter. (Ex: for a key of **1**, **a** would become **b**, **z** would become **a**, etc.)
4. The message should now be encoded.

Decryption

1. Choose the alphabet that the message was encrypted with.
2. Let **n** be the secret key the message is encoded in.
3. For every letter in the cipher-text, replace it by a letter of the alphabet that is **n** letters behind in the alphabet from the letter. **c** would be **b**, **a** would be **z** with a key of **1**.
4. The message should now be decoded

Example

An example of encryption

Let us say we are sending a secret message to a friend.

- We first write out our message. In this case: `The Caesar cipher is a fun substitution cipher`

- Our alphabet will be: `abcdefghijklmnopqrstuvwxyz`. For the uses of this tutorial, case doesn't matter. (On a shift of 1: A will become B, a will become `b`)
- Let our key be 6.
- Starting with the first letter: T. The letter 6 letters away is Z. We add Z to the message.
- The second letter is `h`. The letter 6 letters away is `n`. Our message is now `Zn`
- We continue like that until the end. Our final message is: `Znk Igkygx iovnqx oy g lat yahyzozazout iovnqx`.
- Decryption is the same way, except instead of going to the right in the alphabet, we go backwards.