

GeeksforGeeks

A computer science portal for geeks

Placements

Practice

GATE CS

IDE

Q&A

GeeksQuiz

Login/Register

Caesar Cipher

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions 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 apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

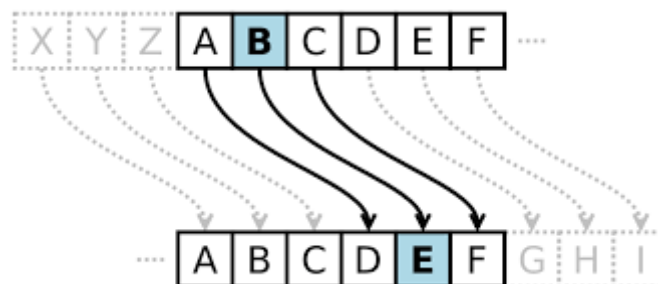
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) \bmod 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) \bmod 26$$

(Decryption Phase with shift n)



Examples :

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift: 23

Cipher: XYZABCDEFGHIJKLMNQPQRSTUVWXYZ

Text : ATTACKATONCE

Shift: 4

Cipher: EXXEGOEXSRGI

Algorithm for Caesar Cipher:**Input:**

1. A String of lower case letters, called Text.
2. An Integer between 0-25 denoting the required shift.

Procedure:

- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
- Return the new string generated.

Program that receives a Text (string) and Shift value(integer) and returns the encrypted text.

C++

```
// A C++ program to illustrate Caesar Cipher Technique
#include <iostream>
using namespace std;

// This function receives text and shift and
// returns the encrypted text
string encrypt(string text, int s)
{
    string result = "";

    // traverse text
    for (int i=0;i<text.length();i++)
    {
        // apply transformation to each character
        // Encrypt Uppercase letters
        if (isupper(text[i]))
            result += char(int(text[i]+s-65)%26 +65);

        // Encrypt Lowercase letters
        else
            result += char(int(text[i]+s-97)%26 +97);
    }

    // Return the resulting string
    return result;
}

// Driver program to test the above function
int main()
{
    string text="ATTACKATONCE";
    int s = 4;
    cout << "Text : " << text;
    cout << "\nShift: " << s;
    cout << "\nCipher: " << encrypt(text, s);
    return 0;
}
```

[Run on IDE](#)**Java**

```
//A Java Program to illustrate Caesar Cipher Technique
class CaesarCipher
{
    // Encrypts text using a shift of s
    public static StringBuffer encrypt(String text, int s)
    {
        StringBuffer result= new StringBuffer();

        for (int i=0; i<text.length(); i++)
        {
            if (Character.isUpperCase(text.charAt(i)))
            {
                char ch = (char)((((int)text.charAt(i) +
                                   s - 65) % 26 + 65));
                result.append(ch);
            }
            else
            {
                char ch = (char)((((int)text.charAt(i) +
                                   s - 97) % 26 + 97));
                result.append(ch);
            }
        }
        return result;
    }

    // Driver code
    public static void main(String[] args)
    {
        String text = "ATTACKATONCE";
        int s = 4;
        System.out.println("Text : " + text);
        System.out.println("Shift : " + s);
        System.out.println("Cipher: " + encrypt(text, s));
    }
}
```

Run on IDE

Python

```
#A python program to illustrate Caesar Cipher Technique
def encrypt(text,s):
    result = ""

    # traverse text
    for i in range(len(text)):
        char = text[i]

        # Encrypt uppercase characters
        if (char.isupper()):
            result += chr((ord(char) + s-65) % 26 + 65)

        # Encrypt lowercase characters
        else:
            result += chr((ord(char) + s - 97) % 26 + 97)

    return result

#check the above function
text = "ATTACKATONCE"
s = 4
print "Text : " + text
print "Shift : " + str(s)
print "Cipher: " + encrypt(text,s)
```

Run on IDE

Output:

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI

How to decrypt?

We can either write another function decrypt similar to encrypt, that'll apply the given shift in the opposite direction to decrypt the original text. However we can use the cyclic property of the cipher under modulo , hence we can simply observe

$$\text{Cipher}(n) = \text{De-cipher}(26-n)$$

Hence, we can use the same function to decrypt, instead we'll modify the shift value such that $\text{shift} = 26 - \text{shift}$ (Refer [this](#) for a sample run in C++).

This article is contributed by **Ashutosh Kumar**. If you like GeeksforGeeks and would like to contribute, you can also write an article and mail your article to contribute@geeksforgeeks.org. See your article appearing on the GeeksforGeeks main page and help other Geeks.

Please write comments if you find anything incorrect, or you want to share more information about the topic discussed above

Company Wise Coding Practice Topic Wise Coding Practice

1 Comment Category: Strings

Related Posts:

- [Check if string follows order of characters defined by a pattern or not | Set 3](#)
- [Check if string follows order of characters defined by a pattern or not | Set 2](#)
- [Find k'th character of decrypted string](#)
- [Minimum Cost To Make Two Strings Identical](#)
- [Find all strings that match specific pattern in a dictionary](#)
- [Check if string follows order of characters defined by a pattern or not | Set 1](#)
- [Find longest palindrome formed by removing or shuffling chars from string](#)
- [Calculate sum of all numbers present in a string](#)

[\(Login to Rate and Mark\)](#)

1.7

Average Difficulty : **1.7/5.0**
Based on **14** vote(s)

Add to TODO List



Mark as DONE

Writing code in comment? Please use code.geeksforgeeks.org, generate link and share the link here.

1 Comment

GeeksforGeeks

 Tejas Joshi ▾ Recommend 1 Share

Sort by Newest ▾



Join the discussion...

**satyam** • 3 months ago

Can u tell me what was the need of
result += char(int(text[i]+s-65)%26 +65) and
result += char(int(text[i]+s-97)%26 +97);

when things can be done by using
result += char(int(text[i]+s))
that too for both upper and lower cases.

^ | ▾ • Reply • Share ›

 Subscribe  Add Disqus to your site Add Disqus Add  Privacy[@geeksforgeeks](#), [Some rights reserved](#)[Contact Us!](#)[About Us!](#)[Advertise with us!](#)