

# Cifra de César: Método Funcional

Raphael Valdetaro

November 2, 2023

## Abstract

Neste artigo, apresentarei minha própria versão da cifra de César, que não depende apenas de uma constante para o deslocamento, mas sim de uma função que altera o deslocamento a cada novo caractere. Isso adiciona uma camada de segurança e complexidade à cifra clássica de César.

## 1 Introdução

A cifra de César é um dos métodos de criptografia mais simples e antigos, que envolve um deslocamento fixo de caracteres no alfabeto. No entanto, nesta versão, estamos introduzindo uma variante que usa uma função para determinar o deslocamento. Vamos explorar como isso funciona e como implementá-lo.

## 2 Definições

Para entender a cifra de César funcional, vamos definir alguns elementos-chave:

$a$  - Uma palavra a ser criptografada.

$f$  - Uma função que determina o deslocamento.

$c$  - Uma constante que afeta a função  $f$ .

$b$  - A palavra criptografada resultante.

## 3 Método Funcional da Cifra de César

O método funcional da cifra de César envolve o uso de uma função  $f$  que define o deslocamento para cada caractere da palavra. A fórmula geral é dada por:

$$b_i = a_i + f(c_i)$$

onde  $b_i$  é o caractere criptografado,  $a_i$  é o caractere original,  $f(c_i)$  é o deslocamento determinado pela função  $f$  com base na constante  $c_i$ .

## 4 Exemplo Prático

Vamos considerar um exemplo prático para ilustrar como a cifra de César funcional funciona. Suponha que tenhamos a palavra "HELLO" e uma função  $f$  que multiplica o valor ASCII de cada caractere por 2. A constante  $c$  é 3.

$$\begin{aligned}a_i &: \text{"HELLO"} \\ f(c_i) &: \text{"CCC"} \quad (\text{com base na função}) \\ b_i &: \text{"KHOOR"} \quad (\text{resultado criptografado})\end{aligned}$$

## 5 Conclusão

A cifra de César funcional oferece uma abordagem interessante para a criptografia, tornando o deslocamento de caracteres dependente de uma função. Isso pode adicionar uma camada adicional de segurança, tornando mais difícil a quebra da criptografia.