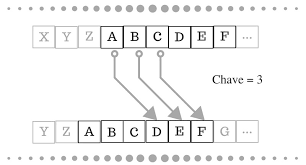
**CIFRA DE CÉSAR**

1. **Estruturação, fundamentos e conceitos**

O uso mais antigo que conhecemos de uma cifra de substituição, e o mais simples foi feito por Júlio César. A Cifra de César é a forma de criptografia mais conhecida no mundo, com propósitos militares, surgiu nas Guerras da Gália de Júlio César, e por este motivo ficou conhecida como Cifra de César. Ela basicamente substituía cada letra na mensagem por outra que estivesse três casas à frente. Mesmo com sua facilidade na época obteve muito sucesso, visto ser analfabeta a maioria dos inimigos do Império Romano, e os poucos que sabiam ler imaginavam que o texto estivesse escrito em outra língua.



Exemplificando a lógica deste método, em um texto criptografado com chave 3, cada letra aumentaria em três posições no alfabeto: ’A’ se tornaria ’D’, ’B’ se tornaria ’E’ e assim por diante. Chegando ao final do alfabeto, ele retornaria ao início, por exemplo, ’Z’ se tornaria ’C’.

A cifra de César usa o que chamamos de criptografia de chave simétrica, onde a mesma chave usada para criptografar o texto é usada também para descriptografar.

O algoritmo pode ser expresso da forma a seguir. Para cada letra em texto claro p, substitua-a pela letra do texto cifrado C2:

C = E (3, p) = (p + 3) mod 26

Um deslocamento pode ser de qualquer magnitude, de modo que o algoritmo de César geral é

C = E(k, p) = (p + k) mod 26 (2.1)

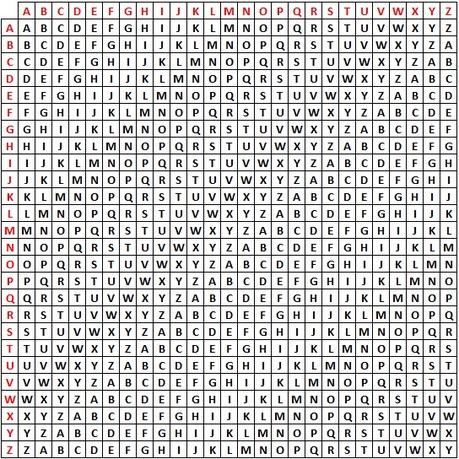
onde k assume um valor no intervalo de 1 a 25. O algoritmo de decriptação é simplesmente

p = D(k, C) = (C – k) mod 26

**1.2 Aplicações com a cifra de César**

1.3 Quadro de Trimethius

Leon Battista Alberti utilizava um quadro composto por 26 linhas e 26 colunas contendo todas as letras do alfabeto, ficando conhecido como Quadro de Trimethius devido ao primeiro livro impresso sobre criptografia “Poligrafia em seis livros por João Trithmius”. Jonathan Strickland explica que um estudioso chamado Johannes Trimethius, se propôs a colocar o alfabeto em uma matriz. A primeira linha continha o alfabeto normalmente escrito. A próxima linha usava uma cifra de César para mover o alfabeto sobre um espaço. Cada linha alterava o alfabeto em um outro ponto para que a linha final iniciasse com a letra “z” e terminasse com a letra “y”. Você poderia ler o alfabeto normalmente olhando para a primeira linha ou pela primeira coluna. Resultando assim:



Jonathan Strickland explica que cada linha é uma cifra de César e que para criptografar uma letra, o criptógrafo escolhe uma linha e usa a primeira linha como guia do texto simples. Um criptógrafo usando a 10ª linha, por exemplo, codificaria a letra de texto simples "a" como "j".

Jonathan Strickland (2007) completa falando que Trimethius sugeriu que os criptógrafos criptografassem suas mensagens usando a primeira linha para a primeira letra, a segunda linha para a segunda letra e assim por diante até o final do quadro. Após chegar ao final, o criptógrafo volta a primeira linha e segue a sequência até criptografar a mensagem toda.

De acordo com Jonathan Strickland (2007) o quadro de Trimethius é um bom exemplo de uma cifra polialfabética. A maioria das cifras antigas eram monoalfabéticas, o que significa que um alfabeto em cifra substitui um alfabeto de texto simples. Uma cifra polialfabética usa múltiplos alfabetos para substituir o texto simples. Apesar das mesmas palavras serem usadas em cada linha, as letras dessa linha têm um significado diferente. Um criptógrafo codifica um texto simples

"A" na linha três como um "C," porém um "A" na linha 23 é um "W". O sistema de Trimethius, no entanto, usa 26 alfabetos - um para cada letra no alfabeto normal.

1.4 Cifra de Vigenère

Está cifra é constituída por 26 cifras de César, com diferentes variações. A diferença é que numa cifra de César, cada letra do alfabeto é deslocada da sua posição um número fixo de lugares, enquanto na cifra de Vigenère consiste de várias cifras de César com diferentes valores de deslocamentos.

Esse método de criptografia foi descrito originalmente pelo criptologista italiano Giovan Battista Bellaso em um livro de 1553 de nome “La cifra del. Sig. Giovan Battista Bellaso”. Curiosamente, o método foi atribuído posteriormente – e de forma errônea – a Blaise de Vigenère no século XIX, e por isso é conhecida até os dias de hoje por “Cifra de Vigenère”. Trata-se basicamente de uma cifra muito simples de entender, implementar e até mesmo quebrar, mas mesmo assim três séculos se passaram até que alguém conseguisse quebra-la.

A cifragem é realizada com o uso de uma tabela de alfabetos, denominada tabula recta, ou “quadrado de Vigenère”, que consiste no alfabeto escrito 26 vezes em linhas diferentes, cada um deslocado ciclicamente para a esquerda comparado com o alfabeto anterior, de forma a corresponder às 26 cifras de César possíveis. Durante o processo de criptografia, a cifra usa um alfabeto diferente de uma das linhas, e o alfabeto a ser utilizado em cada ponto depende da palavra-chave, que é repetida caso a mensagem a ser cifrada seja maior do que ela.

**1.3 Discussão comparativa**

É importante observar o contexto e época de criação da cifra de César para compara-la com outros métodos de criptografia. A cifra de César foi construída de forma extremamente simples comparando com as tecnologias atuais como Advanced Encryption Standard (AES). Entretanto em usos didáticos e para públicos que estão se introduzindo no grandioso mundo dos algoritmos, a cifra de César é um excelente meio para iniciar os estudos.

**1.4 Problemas da cifra de César**

- Possui um número limitado e pequeno de chaves.

- Não permite a autenticação.

- Pode sofrer diversos tipos de criptoanálise.

- Dificuldade de gerenciamento e transmissão de chaves.

**1.5 Formas de aprimorar a cifra de César**