**OBJETIVO GERAL DO TRABALHO**

Pesquisar, analisar e dissertar sobre diversos aspectos das técnicas de criptografia, juntamente com a apresentação de um programa funcional de criptografia.

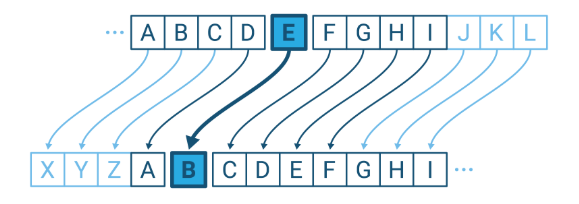
**OBJETIVO ESPECIFÍCO**

Explorar diferentes formas de criptografias através de pesquisas pontuadas, desenvolver com maior veemência a Cifra de César demonstrando usos, aplicações, problemáticas e contextualização. Além disso, conciliar todos os conhecimentos adquiridos elaborando um programa baseado nos conhecimentos anteriormente apresentados.

**CIFRA DE CÉSAR**

1. **Estruturação, fundamentos e conceitos**

A cifra de substituição mais antiga que conhecemos, 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, o que corresponde o tamanho do intervalo de letras que serão puladas: ‘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 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

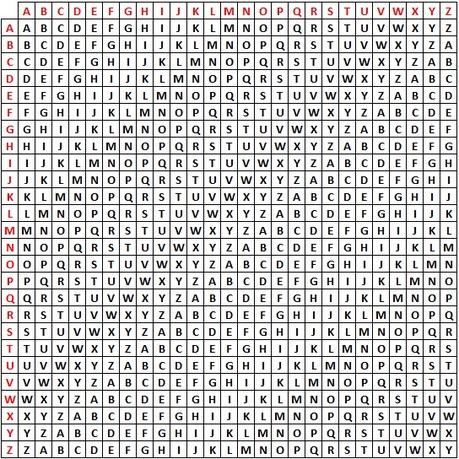
**1.2 Aplicações utilizando da cifra de César**

1.3 Quadro de Trithemius

Os textos criptogrados com substituição monoalfabética se tornaram vulneráveis após AI-Kindi (figura proeminente na Casa da Sabedoria). Mesmo assim, perduraram por algum tempo pois a troca de informações era muita mais lenta nessa época. No século XV, Leon Battista Alberti utilizava um quadro composto por 26 linhas e 26 colunas contendo todas as letras do alfabeto, ficando conhecido como Quadro de Trithemius devido ao primeiro livro impresso sobre criptografia “Poligrafia em seis livros por João Trithemius”.

Jonathan Strickland explica que um estudioso chamado Johannes Trithemius, 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’. Qualquer pessoa poderia ler o alfabeto normalmente olhando para a primeira linha ou pela primeira coluna. Resultando assim:

**Quadro de Trithemius**



**Criptograma**

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’. Strickland completa ainda falando que Trithemius 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.

O quadro de Trithemius é um bom exemplo de uma cifra poli alfabética. 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 Trithemius, no entanto, usa 26 alfabetos - um para cada letra no alfabeto normal.

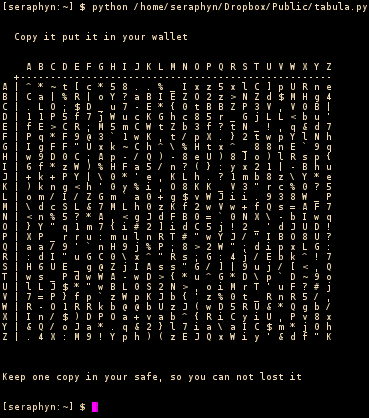
1.4 Cifra de Vigenère

Este tipo de cifra de substituição inventada pelo criptógrafo francês do século XVI Blaise de Vigenère é usada para criptografia de dados em que a estrutura original do texto-planície é um pouco escondida no texto cifrado usando várias diferentes cifras de substituição monoalfabéticas em vez de apenas uma. 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”.

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.

**Tabula Recta**



**Programa em python demonstrando tabula recta**

**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**

Dentre os problemas da cifra de César podemos listar, número limitado e pequeno de chaves, não permitir a autenticação, alta probabilidade de sofrer diversos tipos de criptoanálise e dificuldade de gerenciamento e transmissão de chaves

A cifra de César, portanto, é evidentemente bastante limitada em termos das capacidades de criptografia que pode oferecer. Na era e nos tempos de capacidades extraordinárias de computação, a cifra de César não vale a pena implementar como um esquema de criptografia, simplesmente não é segura. No entanto, a cifra de César ainda pode encontrar seu uso em algumas aplicações triviais, onde a cifra de César poderia ser empregada como um meio simples apenas para obscurecer o significado das mensagens.

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

1.0 Permutação

Nesta abordagem, em vez de mudar as letras linearmente, eles são deslocados aleatoriamente usando a substituição e técnicas de caixa de permutação que são implementadas em técnicas modernas de criptografia como DES.

Então a caixa de substituição deve ser criada implementando a técnica de cifra affine (ou seja, Texto cifrado = (Texto Simples \* chave1) + chave2. Os caracteres são então substituídos por seus valores equivalentes referentes a caixa de substituição. Adicionando a funcionalidade de embaralhar o texto cifrado para esconder as características da linguagem usando técnicas de permutação. A permutação do texto cifrado é feita usando coluna dupla transposição no texto cifrado. O algoritmo proposto pode criptografar a gama de caracteres que a cifra césar não pode criptografar, ou seja, caracteres ASCII e ASCII estendidos.

1. Índice

Neste método, em primeiro lugar, o índice do alfabeto é verificado se o índice do alfabeto é mesmo, então, aumentar o valor por uma outra forma o índice é ímpar diminuir o valor-chave por um. Além disso, os caracteres do texto criptografado são mexidos de tal forma que se uma tentativa é feita para descriptografar o texto cifrado não seria fácil de decifrar.

Passo 1: Tome o texto simples como entrada.

Passo 2: Em primeiro lugar, o índice do alfabeto é verificado se o índice do alfabeto é mesmo, então aumenta-se o valor por mais um ou diminui-se a chave por menos um.

Criptografia:

C=E (P) = (P+1) se P for igual ou zero do que adicionar um

E (P) = (P-1) (mod 26) se p for ímpar do que subtrair um

Descriptografia:

P=D(C) =(C-1) se C for estranho que subtrair um

D(C) = (C+1) se P for igual ou zero do que adicionar

# Bibliografia

A.F., S., & R.M, M. (2018). *cryptograma.blogspot*. Fonte: cryptograma.

Araújo, E. J. (2018). Criptografia dos rudmentos á atualidade. p. 75.

Certificadora, V. (06 de 02 de 2019). *cryptoid*. Fonte: crypto id: https://cryptoid.com.br/valid/tipos-de-criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/

Khandoker Abdul Rahad, Sayed Mohsin Reza . (01 de 2013). A Study on Network Security Services with Cryptography and an Implementation of Vigenere-Multiplicative Cipher.

Rosiane de Freitas, Karla Pereira, Larissa Pessoa e Ariel Bentes. (21 de 04 de 2018). Cifra de Cesar - Princípios de criptografia. p. 9.

Sant´Ana, A. A. (01 de 12 de 2014). Criptografia RSA.

Sarkar, S. (01 de 06 de 2020). Know about the Caesar Cipher. p. 4.

Simmons, G. J. (s.d.). *Britannica*. Fonte: https://www.britannica.com/topic/Vigenere-cipher