INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA – *CAMPUS* ARIQUEMES

MARIA CLARA SANAGIOTO
FELIPE MURILO
MARIA ESTELA

SEGURANÇA DA INFORMAÇÃO: PESQUISA SOBRE A CIFRA DE CÉSAR

Trabalho apresentado ao curso de Informática Integrado ao ensino médio do Instituto Federal de Rondônia (IFRO) como requisito parcial de avaliação da disciplina de Segurança da Informação

ARIQUEMES – RO
2025

SUMÁRIO

1. INTRODUÇÃO..... 2
2. FUNCIONAMENTO DA CIFRA DE CÉSAR..... 2
3. EXEMPLO PRÁTICO..... 2
4. IMPORTÂNCIA E LIMITAÇÕES..... 2
5. CONSIDERAÇÕES FINAIS..... 3
6. REFERÊNCIAS..... 3

1. INTRODUÇÃO

A criptografia é um campo da ciência da computação e da matemática que estuda técnicas para proteger informações contra acessos não autorizados. Um dos métodos criptográficos mais antigos conhecidos é a **Cifra de César**, atribuída a Júlio César, imperador romano. Este trabalho tem como objetivo apresentar o contexto histórico, funcionamento, exemplos e relevância da Cifra de César, destacando suas contribuições para a evolução da criptografia.

A Cifra de César é considerada uma das primeiras técnicas de criptografia registradas. Júlio César (100 a.C – 44 a.C) utilizava este método para enviar mensagens militares de forma que apenas seus aliados conseguissem compreender o conteúdo (KAHN, 1996).

2. FUNCIONAMENTO DA CIFRA DE CÉSAR

O funcionamento baseia-se em um **algoritmo de substituição monoalfabética**, no qual cada letra da mensagem original é substituída por outra letra deslocada no alfabeto. Por exemplo, um deslocamento de 3 posições transforma a letra “A” em “D”, “B” em “E” e assim sucessivamente (STALLINGS, 2017).

3. EXEMPLO PRÁTICO

Um exemplo prático abaixo:

Mensagem: “ME CHAMO FELIPE E SOU UM ESTUDANTE DA REDE FEDERAL”

Mensagem codificada para chave 3: “PH FKDPR IHOLSH H VRX XP HVWXGDQWH GD UHGH IHGHUDO”

4. IMPORTÂNCIA E LIMITAÇÕES

Apesar de sua simplicidade, a Cifra de César é de grande importância histórica por ter introduzido o conceito de criptografia de chave. Contudo, seu uso prático hoje é

extremamente limitado, pois pode ser facilmente quebrada por força bruta ou análise de frequência (BURNETT; PAINE, 2001).

5. CONSIDERAÇÕES FINAIS

A Cifra de César representa o marco inicial da criptografia, trazendo a ideia de proteger informações por meio de substituição sistemática de caracteres. Apesar de suas fragilidades diante das técnicas modernas, seu estudo é essencial para compreender os fundamentos da segurança da informação e a evolução dos algoritmos criptográficos.

6. REFERÊNCIAS

BURNETT, Steve; PAINE, Stephen. *Fundamentos de criptografia aplicada em Java*. Rio de Janeiro: Alta Books, 2001.

KAHN, David. *The codebreakers: the comprehensive history of secret communication from ancient times to the Internet*. New York: Scribner, 1996.

***site112.com*. Disponível em: https://site112.com/cifra-de-cesar-codificar-descodificar. Acesso em: 17 set. 2025.**

STALLINGS, William. *Criptografia e segurança de redes: princípios e práticas*. 7. ed. São Paulo: Pearson, 2017.