

## Criptografia de mensagens utilizando matrizes

**Autores:** Bernardo Benini Fantin, Camila Pâmela Mocellin, Gabriel Lemes Martiori, Caroline Dartora Burkoski Zago, Marco Antônio Ferri

**Orientador:** Hewerton Enes de Oliveira

**Coorientador(es):** Deise Nívia Reisdoefer

A criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra forma ilegível, de modo que possa ser conhecida apenas por seu destinatário. As operações com matrizes podem ser utilizadas para codificar ou decodificar determinada mensagem. Dessa forma, é possível utilizar as operações e propriedades das matrizes para criptografar e descriptografar mensagens. Neste trabalho foi desenvolvido um programa capaz de criptografar e descriptografar uma mensagem de texto utilizando matrizes. Para desenvolver o programa foram realizadas pesquisas bibliográficas com o intuito de adquirir conhecimento sobre as operações e propriedades das matrizes e sua relação com a criptografia. Após, foram desenvolvidos trechos de código para manipular e realizar operações com matrizes utilizando a linguagem de programação Python. Os trechos de código foram agrupados em um módulo permitindo a distribuição do código para qualquer desenvolvedor utilizar. Com o módulo desenvolvido e testado o protótipo do programa foi criado. O programa desenvolvido foi capaz de criptografar uma mensagem de texto transformando-a em uma sequência de números e em seguida descriptografá-la. Foi possível criptografar qualquer mensagem de texto independentemente do tamanho. O método de criptografia utilizado mostrou-se eficiente já que não foi possível quebrar a criptografia utilizando análise estatística. Com o trabalho desenvolvido foi possível concluir que a criptografia é uma forte aliada a disseminação de informações confidenciais, sendo a principal forma de transferência de mensagem em situações que envolvam risco de roubo das informações privilegiadas como nas transferências bancárias e comunicação entre tropas no campo de batalha. O programa desenvolvido foi de crucial importância para o entendimento do assunto e de um método criptográfico

**Palavras-chave:** criptografia, matrizes, programação