

Criptografia de mensagens: uma prática pedagógica entre a Tecnologia da Informação e o Ensino de Matemática

**Beatriz O. Lustosa¹, Bruna C. Steca¹, Yasmim S. Bortese¹,
Maria Eduarda Pereira¹, Eduardo H. Dias¹, Marcelo F. Terenciani¹,
Angela F. Marques¹**

¹Instituto Federal do Paraná (IFPR) Campus Paranavaí
Paranavaí – PR – Brasil

{lustosa.b19, brunasteca, soaresyasmim475}@gmail.com,

{20223020084, 20223019314}@estudantes.ifpr.edu.br,

{marcelo.terenciani, angela.marques}@ifpr.edu.br

A proposta de integrar a Tecnologia da Informação (TI) ao ensino de Matemática surge como uma resposta à necessidade de inovação e engajamento nas práticas pedagógicas. Em um cenário em que os estudantes têm uma interação cada vez maior com a tecnologia, é essencial que os processos de ensino e de aprendizagem acompanhem essa evolução. Conforme [Diniz 2001], existem diversos desafios no uso da tecnologia no ensino da Matemática. Um dos principais é a criação de espaços de aprendizagem que possibilitem aos estudantes vivenciar situações que se conectem com sua realidade, promovendo uma maior interação com os conteúdos abordados. Outro desafio importante é incentivar os alunos a estabelecer relações entre os diferentes conhecimentos, manipulando os conceitos sempre que possível ou associando-os aos conteúdos previamente estudados.

A Matemática, muitas vezes considerada uma disciplina abstrata e distante da realidade dos estudantes, pode sofrer inovações e ganhar novo significado quando associada ao uso de tecnologias práticas. Para [Rossi and Bisognin 2010], às inovações tecnológicas no ensino de Matemática configuram uma verdadeira revolução na forma como essa disciplina é ensinada e aprendida. Essas inovações englobam desde ferramentas digitais interativas até metodologias de ensino fundamentadas em dados, com o objetivo de tornar o aprendizado da Matemática mais dinâmico, eficiente e acessível.

A criptografia é um exemplo de como a Matemática pode ser aplicada de forma concreta e relevante. Ao utilizar conceitos como matrizes e determinantes para criptografar mensagens, busca-se proporcionar aos alunos uma compreensão profunda de um conceito essencial para a segurança da informação, tornando o ensino de conteúdos abstratos mais interativo e aplicado.

O objetivo central da proposta é promover a integração da Tecnologia da Informação e o Ensino de Matemática, utilizando a criptografia como ferramenta para o ensino de conceitos matemáticos como matrizes e determinantes. A ideia é que os estudantes não apenas aprendam a teoria desses conteúdos, mas também desenvolvam habilidades práticas ao criar e implementar um programa ou aplicativo capaz de codificar e decodificar mensagens. Essa abordagem permite que os alunos se envolvam de forma ativa na construção de seu conhecimento, estimulando a compreensão dos conteúdos e a aplicação prática das habilidades adquiridas.

A criptografia é o processo de codificar uma mensagem para que ela seja transmitida de forma segura, impedindo que pessoas não autorizadas possam acessá-la. A segurança da informação é um aspecto fundamental na sociedade contemporânea, seja em transações bancárias, comunicações pessoais ou empresariais, e a criptografia desempenha um papel crucial nesse contexto. Em termos matemáticos, a criptografia envolve transformações que dificultam a leitura de mensagens sem o uso de uma chave específica, e muitas dessas transformações podem ser modeladas por operações com matrizes e determinantes.

As primeiras formas de criptografia datam de tempos antigos, mas foi durante o século XX, com o advento da computação, que a criptografia passou a ser utilizada de maneira mais sofisticada e amplamente aplicada. As matrizes, especificamente, têm sido empregadas em diversos algoritmos criptográficos, como no método de cifra de Hill, que utiliza operações com matrizes para cifrar e decifrar mensagens. Assim, as matrizes e determinantes se apresentam como uma excelente oportunidade para o ensino de Matemática, ao mesmo tempo que se conecta com uma aplicação prática relevante na sociedade atual.

Matrizes são arranjos bidimensionais de números que podem ser usados para representar uma série de operações matemáticas. No contexto da criptografia, elas permitem a transformação de dados de maneira sistemática, o que facilita a criação de algoritmos de codificação e decodificação. Determinantes, por sua vez, são números associados a matrizes que possuem diversas propriedades importantes, como a possibilidade de determinar se uma matriz é invertível — algo essencial em muitos sistemas criptográficos.

O desenvolvimento de um programa ou aplicativo que permite a codificação e decodificação de mensagens com matrizes envolve o uso de linguagens de programação, como Python ou JavaScript, que oferecem bibliotecas e funcionalidades para manipulação de matrizes e operações matemáticas. Os alunos são incentivados a construir esse software de maneira colaborativa, dividindo tarefas e discutindo soluções. Ao criar o programa, os estudantes não só aplicam os conceitos matemáticos de matrizes e determinantes, mas também desenvolvem habilidades em programação, lógica computacional e resolução de problemas.

O programa/aplicativo surgiu pela necessidade de resolver o problema: Usem sua criatividade para inventar uma mensagem e depois criptografá-la, usando os conteúdos de matrizes, determinantes e matriz inversa. Transmita sua mensagem codificada e desafie outras pessoas para decifrá-la apenas sabendo como você a codificou, ou seja, não diga a eles, de início, como decodificar a mensagem.

A metodologia adotada visa promover uma aprendizagem ativa, centrada no aluno. Os estudantes são desafiados a explorar o conteúdo de maneira prática, aplicando os conceitos de matrizes e determinantes no desenvolvimento do programa de criptografia. As etapas da metodologia incluem:

- **Introdução ao Conteúdo Matemático:** O professor trabalha os conceitos de matrizes e determinantes, abordando suas propriedades e aplicações;
- **Exploração da criptografia:** O conceito de criptografia é introduzido, explicando sua relevância e como ela pode ser modelada matematicamente com o uso de matrizes;

- **Desenvolvimento do Programa:** Os alunos trabalham em grupos para criar um programa que permita a codificação e decodificação de mensagens, utilizando as operações com matrizes;
- **Testes e Validação:** Os alunos testam o programa com diferentes entradas e verificam a eficácia da criptografia, ajustando o código conforme necessário;
- **Reflexão e Discussão:** Ao final do projeto, os alunos discutem o que aprenderam, as dificuldades encontradas e a importância dos conceitos matemáticos no mundo real.

A proposta enfatiza a aprendizagem colaborativa, o uso de tecnologias para resolver problemas matemáticos e a construção ativa de conhecimento, o que contribui para uma maior compreensão e retenção do conteúdo pelos alunos. Para [Rêgo 2016], o potencial das tecnologias para enriquecer e aprimorar o aprendizado da Matemática é indiscutível, uma vez que elas estão abrindo novas possibilidades para uma compreensão mais profunda e um maior apreço pela disciplina, habilidades essenciais no mundo moderno.

Ao final da proposta, espera-se que os estudantes compreendam profundamente os conceitos de matrizes e determinantes, além de perceberem suas aplicações na segurança da informação. Integrar a Tecnologia da Informação ao Ensino de Matemática, utilizando conceitos matemáticos na criptografia, oferece uma abordagem inovadora e eficaz para o aprendizado. Ao aplicar matrizes e determinantes na codificação e decodificação de mensagens, os estudantes não só aprofundam seus conhecimentos matemáticos, mas também se envolvem ativamente na criação de soluções tecnológicas. Essa metodologia, além de fortalecer a compreensão dos conteúdos, favorece o desenvolvimento de habilidades como pensamento crítico, resolução de problemas e proficiência em TI.

Referências

- Diniz, S. N. d. F. (2001). O uso das novas tecnologias em sala de aula. Dissertação (Mestrado em Engenharia de Produção), Universidade Federal de Santa Catarina, Florianópolis, Brasil. 186 f.
- Rossi, G. d. R. and Bisognin, E. (2010). Explorando arte e geometria num ambiente computacional. In *Encontro Nacional de Educação Matemática*, Bahia, Brasil. SBEM.
- Rêgo, A. F. C. d. B. (2016). As novas tecnologias utilizadas no processo de ensino aprendizagem por professores de matemática de escolas públicas no município de limoeiro-pe. In *Encontro Nacional de Educação Matemática*, 12, São Paulo, Brasil. SBEM.