Revista Matemática, Ensino e Cultura

e-ISSN: 2675-1909 | ISSN: 1980-3141
N. 43, e2023034
10.37084/REMATEC.1980-3141.2023.n43.pe2023034.id516

A criptografia no ensino de matrizes na Educação Básica

The cryptography in teaching matrices in Basic Education

La criptografía en la enseñanza de matrices en la Educación Básica

Sávio dos Reis Ferreira[1]

Suellen Cristina Queiroz Arruda[2]

RESUMO

O presente trabalho propõe uma alternativa metodológica ao ensino de matrizes baseada na utilização da criptografia, possibilitando uma abordagem diferenciada das comumente aplicadas em sala de aula. A partir dos processos de codificação e decodificação de mensagens, buscou-se proporcionar um ensino contextualizado de matrizes aos alunos do terceiro ano do Ensino Médio da rede pública de ensino, no município de Belém/PA. Com uma abordagem qualitativa, a pesquisa utilizou um questionário avaliativo da oficina matemática desenvolvida na escola. Os resultados mostram que a aplicação da criptografia auxilia no entendimento dos conceitos básicos de matrizes de uma forma dinâmica e interessante.

Palavras-chave: Criptografia; Matrizes; Ensino; Educação Básica.

ABSTRACT

This paper proposes a methodological alternative to teaching matrices based on the use of cryptography, in order to make possiblea different approach from those commonly applied at in the classroom. From the codification and decoding processes of messages, we sought to provide a contextualized teaching of matrices to third-year high school students from the public school system in the municipality of Belém/PA. With a qualitative approach, the research used an evaluative questionnaire from a mathematical workshop developed in the school. The results show that the application of cryptography helps to understand the basic concepts of matrices dynamically and interestingly.

Keywords: Cryptography; Matrices; Teaching; Basic Education.

RESUMEN

El presente trabajo propone una alternativa metodológica a la enseñanza de matrices basada en el uso de la criptografía, que permita un enfoque diferente a los comúnmente aplicados en el aula. A partir de los procesos de codificación y decodificación de mensajes, buscamos proporcionar una enseñanza contextualizada de las matrices a los alumnos del tercer año de la enseñanza media del sistema escolar público, en la ciudad de Belém/PA. Con un enfoque cualitativo, la investigación utilizó un cuestionario evaluativo del taller matemático desarrollado en la escuela. Los resultados muestran que la aplicación de la criptografía ayuda a comprender los conceptos básicos de las matrices de una forma dinámica e interesante.

Palabras clave: Criptografía; Matrices; Enseñanza; Educación Básica

1 Mestrando em Matemática e Estatística da Universidade Federal do Pará (UFPA), Belém, Pará, Brasil. Endereço para correspondência: Rua Primeira de Queluz, Tv. Santo Antônio, 22 A, Apto 7, São Brás, Belém, Pará, Brasil, CEP: 66090-420. E-mail: savioreis19@mail.com.

2 Doutorado em Matemática pela Universidade Federal do Pará (UFPA). Docente do curso de Licenciatura em Matemática na Universidade Federal do Pará (UFPA), Campus Universitário de Abaetetuba, Abaetetuba, Pará, Brasil. Endereço para correspondência: Passagem Gaspar Dutra, 77, Curió-Utinga, Belém, Pará, Brasil, CEP: 66610-250. E-mail: scqarruda@ufpa.br.

CC BY NC ND

INTRODUÇÃO

A criptografia surgiu como uma maneira de codificar as mensagens, tornando-as secretas. Um dos primeiros códigos descobertos foi o famoso código de César, usado pelo ex-ditador romano Júlio César para conquistar territórios pela Europa e transformar Roma em um império. Para Bezerra, Malagutti e Rodrigues (2010, p. 1), "a importância de não revelar segredos e estratégias às forças inimigas, motivou o desenvolvimento de códigos, cifras e técnicas para mascarar uma mensagem, possibilitando apenas ao destinatário ler o conteúdo".

Com o advento da tecnologia, a criptografia se conceitua como um recurso tecnológico utilizado para enviar mensagens de forma cifrada ou codificada, permitindo que apenas seu emissor e seu receptor tenham acesso ao conteúdo das mensagens criptografadas. Um dos seus princípios é usar seus mecanismos e suporte de segurança digital como ferramenta principal para proteção de dados e informações sigilosas de interesses individuais ou coletivos.

> A tecnologia e o interesse na proteção de dados evoluíram ao longo dos séculos, todavia o grande impulsionador foi certamente o advento do computador, que introduziu uma nova realidade em termos de volume e guarda de dados. Diante deste novo cenário, a tecnologia para a proteção de dados, especialmente no campo da criptografia simétrica (chave única), foi responsável pelo surgimento de soluções que garantem a inviolabilidade dos dados, mesmo contra o uso do computador (ZANCANELLA, 2021, [s.p.]).

No âmbito educacional, verifica-se a contribuição da criptografia no processo de ensino e aprendizagem de Matemática, pois consegue aguçar o interesse e a curiosidade dos alunos, visto que a abordagem serve como uma motivação para fomentar a pesquisa sobre a temática e proporciona abordar conteúdos matemáticos de forma contextualizada com a realidade dos estudantes, conforme descreve Rosseto (2018) no seguinte trecho:

> Usando a criptografia como ferramenta no ensino da Matemática, atribuímos significado ao conceito estudado, de forma que o aluno se sinta motivado a aprendê-lo. Assim, ressaltamos a importância de inserir o uso de assuntos ligados à realidade do aluno, que estimulem o empenho dos mesmos nas aulas, contribuindo de forma significativa para sua aprendizagem (p. 58).

De acordo com Viviani e Costa (2010, p. 50-51), uma das dificuldades no processo de ensino e aprendizagem, e que de alguma forma pode comprometê-lo, é "a falta de atividades práticas e a aproximação dos conteúdos abordados com a realidade dos alunos". Nesse contexto, o presente trabalho consiste na execução de uma oficina matemática a alunos do terceiro ano da Escola Estadual de Ensino Médio Augusto Meira com o intuito de possibilitar uma melhor compreensão de matrizes por meio da criptografia.

Justificamos a escolha do assunto matrizes por dois motivos: primeiro, porque observamos que o conteúdo matemático já havia sido ministrado pelo regente da sala, e segundo, pelo fato do conteúdo ainda ser ministrado de forma tradicional nas escolas, sem trazer, na maioria das vezes, exemplos contextualizados de sua aplicação, o que acaba gerando falta de interesse dos alunos por conta do alto grau de abstração dos conceitos, acarretando assim dificuldades no entendimento do assunto.

Assim, conjugamos que criptografia associada ao ensino de matrizes possibilita que o aluno tenha conhecimento da importância de aprender matrizes para relacionar situações reais presentes na sociedade, seja na criação de senhas criptografadas ou no uso de códigos em guerras. Desta forma, o principal objetivo da oficina matemática é propor atividades baseadas no uso da criptografia de modo a despertar interesse do participante em estudar os conceitos e operações envolvidas no ensino de matrizes.

O trabalho está organizado da seguinte forma: na primeira seção, apresentam-se alguns fatos históricos sobre a criptografia, seu conceito e importância nos dias atuais. Na segunda seção, evidenciam-se as potencialidades do uso da criptografia no ensino da Matemática, em especial no processo de ensino e aprendizagem de matrizes, na perspectiva de tornar as aulas mais atrativas ao trabalhar os conceitos matemáticos. A terceira seção é destinada à descrição da oficina matemática realizada com os alunos do Ensino Médio. Por fim, na última seção, faz-se a apresentação e a discussão dos resultados obtidos através do questionário avaliativo aplicado após a oficina.

UM BREVE HISTÓRICO DA CRIPTOGRAFIA

A palavra criptografia deriva do grego *kryptos*, que significa secreto, oculto. A criptografia tem como objetivo codificar uma mensagem para que apenas o seu destinatário tenha acesso e consiga decodificá-la.

> A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos ‹códigos secretos', que todos já praticamos quando criança. O mais simples destes códigos consiste em substituir uma letra pela seguinte; isto é transladar o alfabeto uma casa para diante (COUTINHO, 2005, p. 1).

A cifra de César é um dos mais antigos e conhecidos desses métodos, datado aproximadamente em 60 a.C., foi criado por Júlio César durante seu governo militar, com o intuito de se comunicar com seus soldados e integrantes das corporações militares. O método utilizado no referido código é a substituição monossilábica, que consiste em uma reorganização das letras do alfabeto em que as mesmas são deslocadas. Portanto, isso faz com que seja muito simples e fácil de ser decifrado.

> A cifra de César é uma técnica de criptografia bastante simples e provavelmente a mais conhecida de todas. Trata-se de um tipo de cifra de substituição, na qual cada letra de um texto a ser criptografado é substituída por outra letra, presente no alfabeto, porém deslocada um certo número de posições à esquerda ou à direita. A cifra de César recebe esse nome, pois, segundo o escritor Suetônio, foi utilizada por Júlio César para se comunicar com seus generais, protegendo mensagens militares (REIS, 2016, [s.p.]).

A cifra de Vigenère, desenvolvida pelo criptologista italiano Giovan Batista Bellaso, em 1553, atribuída erroneamente a Blaise de Vigenère, utiliza várias combinações da cifra de César, baseando-se na substituição polialfabética, ou seja, na substituição múltipla de alfabetos. Com este método de criptografia, é possível melhorar a cifra de César tornando-a mais segura e complexa. Ao longo de três séculos, a cifra de Vigenère se manteve inquebrável, chegando a receber a alcunha de "Le chiffre indéchiffrable" (A cifra indecifrável, em francês). Em meados de 1854, Charles Babbage elaborou a quebra da cifra de Vigenère, po-

rém o desenvolvimento da decodificação dessa valiosa cifra não foi suficientemente eficaz, tornando-se completa somente no ano de 1863 pelo criptógrafo e arqueólogo Friedrich Wilhen Kassiski.

> Para criptografar uma mensagem utilizando a Cifra de Vigenère, o primeiro passo é montar a grelha de Vigenère, um alfabeto normal seguido de 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior. O remetente da mensagem pode, por exemplo, cifrar a primeira letra de acordo com a linha 5, a segunda de acordo com a linha 14 e a terceira de acordo com a linha 21, e assim por diante. Esse sistema deve ser previamente combinado entre remetente e destinatário (BRANDÃO, 2017, p. 51).

Outro método de criptografia bastante conhecido é a Cifra de Hill, desenvolvido pelo matemático norte-americano Lester S. Hill, em 1929, o qual consiste em um tipo de cifra de substituição tendo como suporte conteúdos estudados em Álgebra Linear. Segundo Brandão (2017),

> A cifra de Hill consiste em um sistema de criptografia por substituição polialfabética, baseado em transformações matriciais. Para a aplicação de tal cifra, é necessário criar uma relação biunívoca entre as letras do alfabeto e um subconjunto dos números inteiros (p. 53).

Um marco importante na história da criptografia foi o estudo do francês Jean François Champollion para decifrar os códigos antigos da famosa Pedra de Roseta, levada para a França como espólio de guerra, mas que, atualmente, está exposta no Museu Britânico, em Londres. A Pedra de Roseta está escrita em três línguas e sua tradução foi importante tanto para compreensão da história do Egito Antigo quanto para entender como o uso da criptografia está presente há muito tempo na sociedade.

> Nenhuma pedra é tão famosa quanto a de Roseta. O fragmento de um bloco que pesa quase 1 tonelada, mede 118 centímetros, tem 77 centímetros de largura e 30 de espessura, foi fundamental para a compreensão da história do Egito Antigo. O objeto, encontrado na cidade de Roseta, próxima à Alexandria, pelo exército de Napoleão, em 1799, tem uma mensagem escrita em três línguas: hieróglifos, demótico e grego. A pedra virou o trabalho da vida do linguístico francês Jean-François Champollion, que também era professor de história, o que facilitou a missão. Ele trabalhou na tradução de 1822 e 1824, comparando as três línguas para transcrever o decreto. Com isso, conseguiu uma espécie de "chave mestra" para traduzir muitos outros documentos encontrados (REVISTA GALILEU, 2021, [s.p.]).

Como se pode observar, a criptografia vem sendo utilizada há bastante tempo como uma ferramenta de comunicação e informação, tendo grande importância em momentos cruciais na história da humanidade, como, por exemplo, a Segunda Guerra Mundial.

A criptografia na época da Segunda Guerra Mundial foi necessária para envio e recebimento de mensagens secretas entre os comandos militares e seus aliados, presente em códigos e linguagens sigilosas, além do uso de máquinas para codificar e decodificar os códigos de guerra.

> Com a Segunda Guerra Mundial, consolidou-se a importância da informação e da criptografia. O volume de troca de mensagens e a necessidade da criptografia fez com que surgissem as primeiras máquinas de codificação. O exército alemão dispunha de uma máquina, conhecida como Enigma, cujo número de combinações gerado era da ordem de 15×10^{18}, o que a tornava praticamente impossível de ser quebrada. As

> cifras da Enigma foram quebradas por outra máquina, a Enigma Bomb, desenvolvida por Alan Turing. Com a quebra da Enigma os aliados ganham vantagem estratégica e vencem a Segunda Guerra (BRUNO, 2017, [s.p.]).

Após as repercussões da Segunda Guerra Mundial, a criptografia passa a ter um papel fundamental no desenvolvimento de computadores digitais e consequentemente da Internet, dando início à era da Criptografia Computacional. Com o avanço tecnológico, a criptografia dá origem a uma importante ciência, a Criptologia, e ganha novas utilizações em vários contextos importantes na sociedade voltados a aspectos de segurança, tais como: sigilo em bancos de dados, aplicativos de comunicação e informações de crédito pessoal, conforme relatam Bezerra, Malagutti e Rodrigues (2010):

> Hoje em dia, entretanto, com o advento da comunicação eletrônica, a criptografia deixou de ser unicamente segredo de estado, pois muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da Internet. Até recentemente, a criptografia era considerada uma arte; hoje em dia, entretanto, passou a ser considerada uma ciência. As aplicações da Criptografia atualmente incluem: sigilo em banco de dados; censos; investigações governamentais; dossiês de pessoas sob investigação; dados hospitalares; informações de crédito pessoal; decisões estratégicas empresariais; sigilo em comunicação de dados; comandos militares; mensagens diplomáticas; operações bancárias; comércio eletrônico; transações por troca de documentos eletrônicos (EDI); estudo de idiomas desconhecidos; recuperação de documentos arqueológicos, hieróglifos; e até tentativas de comunicações extraterrestres (p. 2).

Portanto, a criptografia é de extrema importância para a humanidade e sua evolução ao longo dos tempos, desde a época da Grécia antiga até os dias atuais, provocando grandes transformações nas formas de transmitir mensagens, garantindo privacidade e proteção nas comunicações.

MATRIZES E CRIPTOGRAFIA

O professor, no uso de uma didática que busca conectar os conteúdos matemáticos com situações presentes no cotidiano, possibilita a construção do conhecimento a partir da constatação da importância da Matemática para o indivíduo, estimulando, assim, uma aprendizagem mais significativa e a democratização do conhecimento.

Tal prática docente está alinhada com as finalidades do Ensino Médio, de acordo com os seguintes trechos da Lei de Diretrizes e Bases da Educação Nacional (LDB):

> O aprimoramento do educando como pessoa humana, incluindo a formação ética e o desenvolvimento da autonomia intelectual e do pensamento crítico; a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, no ensino de cada disciplina; a preparação básica para o trabalho e a cidadania do educando, para continuar aprendendo, de modo a ser capaz de se adaptar com flexibilidade a novas condições de ocupação ou aperfeiçoamento posteriores (BRASIL, 1996, Art. 35. II, III, IV).

Com o avanço da tecnologia, a criptografia passou a ser usada de forma rotineira pelas pessoas, seja na criação de uma senha bancária ou na comunicação pessoal, como, por exemplo, na troca de e-mail ou mensagens via WhatsApp. Nesse sentido, a criptografia surge como uma alternativa metodológica no ensino da Matemática, uma vez que a sua

aplicabilidade, em vários contextos ligados à tecnologia, além de despertar o interesse e curiosidade dos alunos em desvendar o mundo da criptografia, possibilita uma nova forma de ensinar conteúdos matemáticos a partir da contextualização de situações-problema presentes no cotidiano da sociedade, conforme é apontado por Arinos (2014),

> Sabemos que a matemática enfrenta diversos desafios na busca de ligar o interesse discente e a formação do cidadão, partindo do pressuposto de que a educação se concretiza nesta relação. Portanto, aproximar a linguagem matemática da realidade é o foco de estratégias educacionais, para que os alunos se tornem cidadãos conscientes, apropriando-se de conhecimentos matemáticos fundamentais para uma formação crítica de nossa sociedade. Nesse contexto, a criptografia pode ser um elemento motivador para o processo de ensino e aprendizagem da matemática, pois seu desenvolvimento histórico e sua aplicabilidade disponibilizam ao professor muitos exemplos contextualizados, ao mesmo tempo em que promovem uma interessante ligação com as ciências sociais e sociedade (p. 43).

Abordar a criptografia na Educação Básica por meio do método de codificação e decodificação aplicado a matrizes, evidencia a importância de trabalhar o assunto de modo que os discentes possam perceber como é empregado os conceitos ensinados nas aulas de Matemática. Partindo desse pressuposto, a aplicação da criptografia no ensino de matrizes soma e enriquece o processo de aprendizagem dentro da sala de aula, ao apresentar o quão vasto e importante é o seu estudo.

Além disso, a utilização da criptografia proporciona dinâmica na construção do conhecimento matemático, uma vez que seu ensino sai da prática monótona ainda adotada por muitos professores no ensino tradicional, os quais tornam o seu estudo cansativo e desinteressante, fato este mencionado por Moura (2018):

> A criptografia pode ser usada como ferramenta para enriquecer o ensino da matemática, pois sua aplicabilidade abrange os diferentes níveis de ensino e auxilia no desenvolvimento de competências de leitura e escrita por meio da história, além de colaborar com a interdisciplinaridade e principalmente tornar o aprendizado mais significativo (p. 47).

Assim, o ensino de matrizes através da criptografia torna-se uma abordagem de grande importância e utilidade tanto aos alunos quanto ao professor, por se tratar de uma metodologia que possibilita o desenvolvimento científico e a busca por novos desafios para resolução de problemas matemáticos. Segundo Tamarozzi (2001),

> O tema Criptografia possibilita o desenvolvimento de atividades didáticas envolvendo os conteúdos de matrizes e funções que se constituem em material útil para exercícios, atividades e jogos de codificação, onde o professor pode utilizá-los para fixação de conteúdos matemáticos (p. 41).

É importante mencionar que as técnicas criptográficas são fundamentadas em alguns ramos da Matemática, tais como a Álgebra Linear e a Teoria dos Números. De acordo com Druck, Hellmeister e Peixoto (2004),

> Uma das maneiras de manifestação da Criptografia no ensino da matemática é vista no estudo de Álgebra Matricial. Para isso utilizando meios como a multiplicação de Matrizes e Matrizes Invertíveis como chaves, o que faz dificultar a violação da mensagem (p. 71).

Diante disso, ao adotar um método em que o processo de codificação e decodificação de mensagens utiliza matrizes, a criptografia se torna uma ferramenta de ensino significativa no processo de ensino e aprendizagem do conteúdo matemático atrelado, possibilitando ao aluno aprender com maior facilidade, por meio de técnicas que demonstrem o que está presente em seu cotidiano, e ao docente uma nova abordagem de ensinar o assunto em sala de aula.

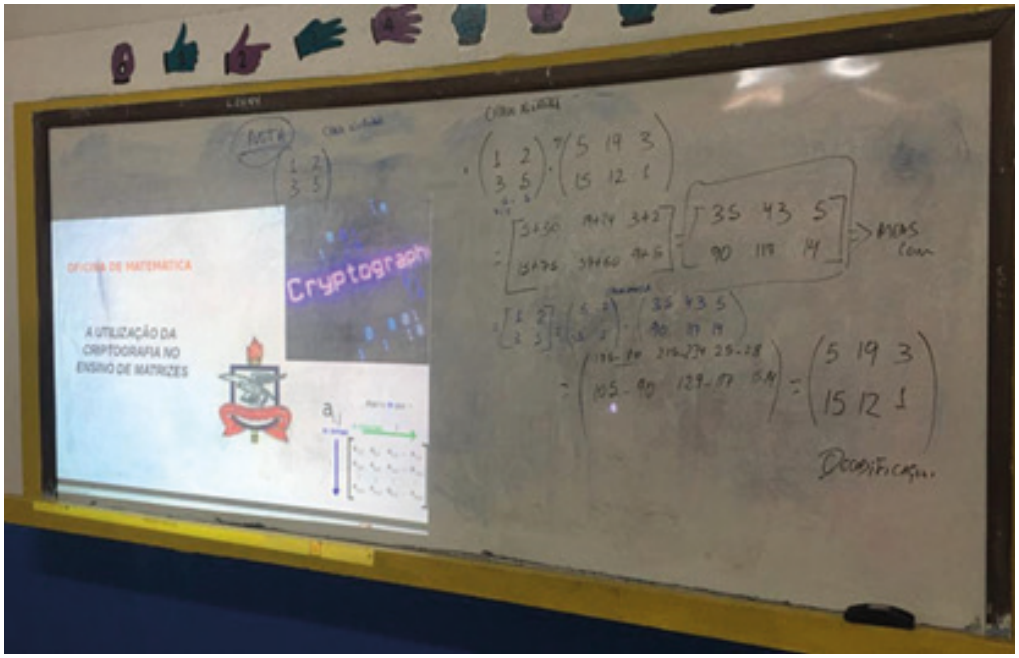
PROCEDIMENTOS METODOLÓGICOS

Trata-se de uma pesquisa com características qualitativas que de acordo com Godoy (1995, p. 21) "não se apresenta como uma proposta rigidamente estruturada, ela permite que a imaginação e a criatividade levem os investigadores a propor trabalhos que explorem novos enfoques" e também exploratórios.

Para alcançar o objetivo de possibilitar uma melhor compreensão de matrizes por meio da criptografia, elaborou-se a oficina "A utilização da criptografia no ensino de matrizes", a ser aplicada a alunos do 3º ano do Ensino Médio da Escola Estadual de Ensino Médio Augusto Meira, no município de Belém, no estado do Pará. De um modo geral, em termos metodológicos, foi adotada uma dinâmica que permitia, durante a atividade, combinar fases de problematização (questionamentos), realização (construções e explorações nas construções das matrizes fazendo uso da criptografia), discussão a partir das produções dos estudantes e a sistematização da oficina.

Antecipadamente, a proposta da oficina foi apresentada a um professor de Matemática da escola, que, gentilmente, cedeu algumas aulas em 4 (quatro) turmas para a realização da intervenção metodológica. A oficina foi elaborada a partir das informações dadas pelo docente sobre os tópicos de matrizes trabalhados nas turmas.

Figura 1. Foto com o título da oficina exposto no quadro.



Fonte: Acervo da pesquisa (2022).

No primeiro momento da oficina, em cada turma, perguntou-se aos alunos se eles sabiam o que era criptografia. A maioria dos alunos respondeu que não sabia do que se tratava, e os poucos que responderam algo, falaram que tinha a ver com aplicativos de mensagens ou internet. Com estas respostas, o conceito de criptografia foi introduzido evidenciando a sua relevância para a sociedade, ao exemplificar sua aplicabilidade na segurança de dados e informações confidenciais.

Dando continuidade, abordou-se o papel de grande importância da criptografia no século XX, durante as guerras que o mundo presenciou. Para despertar o interesse e a curiosidade dos estudantes em saber mais sobre o uso da criptografia, nestes momentos históricos da humanidade, alguns filmes foram sugeridos, a saber: Códigos de Guerra, com Nicolas Cage; The Gray Man, com Ryan Gosling e Chris Evans; e O Jogo da Imitação, com Benedict Cumberbatch.

Para abordar que a necessidade de enviar mensagens com segurança é algo muito antigo, informou-se que na Grécia Antiga o ex-ditador Júlio César utilizava um sistema de substituição monoalfabética para se comunicar com os seus aliados de guerra, ficando conhecido como "cifra de César" e sendo considerado um dos mais antigos métodos criptográficos que se tem registro.

No entanto, enfatizou-se que o processo de codificação das mensagens utilizava somente as 26 letras do alfabeto e, com o passar do tempo, perceberam que a cifra era muito simples e fácil de ser quebrada.

Figura 2. Imagem de um dos slides utilizados na apresentação da oficina.

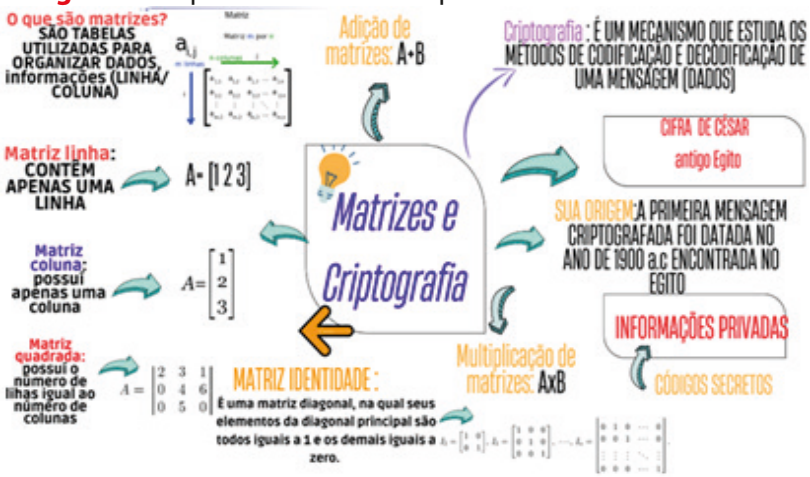
Fonte: Acervo da pesquisa (2022).

Em seguida, explicou-se que para aplicar a criptografia no ensino de matrizes, por meio da criptografia, era necessário relembrar alguns tópicos sobre o assunto matemático. Dito isso, foram explanados o conceito e os elementos de uma matriz, dando alguns exemplos para a classificação de matriz linha, matriz coluna, matriz identidade e matriz quadrada.

Além disso, abordou-se as operações com matrizes, principalmente a multiplicação entre matrizes, e matriz inversa.

Depois da exposição do conteúdo matemático, foi disponibilizado um mapa mental com intuito de ressaltar o conhecimento até então explorado na oficina, conforme a Figura 3.

Figura 3. Mapa mental com os tópicos abordados na oficina.



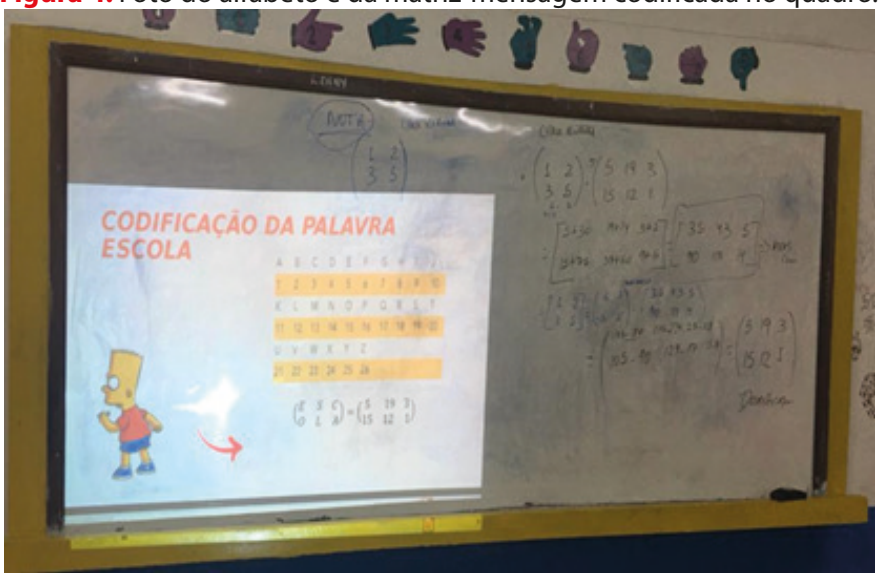
Fonte: Acervo da pesquisa (2022).

No segundo momento da oficina, introduziu-se a atividade elaborada para relacionar matrizes e criptografia. Inicialmente, tratou-se da cifra de Hill, explicando que o processo de codificação e decodificação utiliza uma tabela com as letras do alfabeto enumeradas de 1 (um) a 26 (vinte e seis), conforme mostra a Figura 4, e uma chave aleatória para codificação cujo propósito é proteger ainda mais a mensagem a ser transmitida.

A chave aleatória deve ser de conhecimento apenas do remetente e do destinatário da mensagem. Feito isso, realizou-se os seguintes passos com os alunos:

> **1º Passo**: Dada a palavra ESCOLA para ser codificada, a partir da posição de cada letra no alfabeto, encontrou-se a matriz-mensagem
>
> $$M = \begin{pmatrix} 5 & 19 & 3 \\ 15 & 12 & 1 \end{pmatrix}$$

Figura 4. Foto do alfabeto e da matriz-mensagem codificada no quadro.



Fonte: Acervo da pesquisa (2022).

2º Passo: Para proteger ainda mais a mensagem, a chave dada para codificação foi a matriz

$$C = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$$

Ao realizar a multiplicação entres as matrizes C e M, nesta ordem, encontrou-se a seguinte matriz com a mensagem codificada

$$P = \begin{pmatrix} 30 & 69 & 10 \\ 55 & 119 & 17 \end{pmatrix}$$

Neste momento, enfatizou-se os tópicos necessários sobre matrizes para a obtenção da matriz . Além disso, para a realização da atividade, permitiu-se aos alunos o uso da calculadora no aparelho celular.

3º Passo: Para fazer a decodificação da mensagem, efetuou-se uma nova multiplicação entre matrizes, desta vez utilizando a matriz inversa da chave aleatória e a matriz com a mensagem codificada. Assim, ao calcular $C^{-1}P$, a seguinte matriz foi obtida

$$\begin{pmatrix} 5 & 19 & 3 \\ 15 & 12 & 1 \end{pmatrix}$$

E, assim, conclui-se que a matriz resultante é a matriz M, a qual sabe-se que corresponde à palavra ESCOLA.

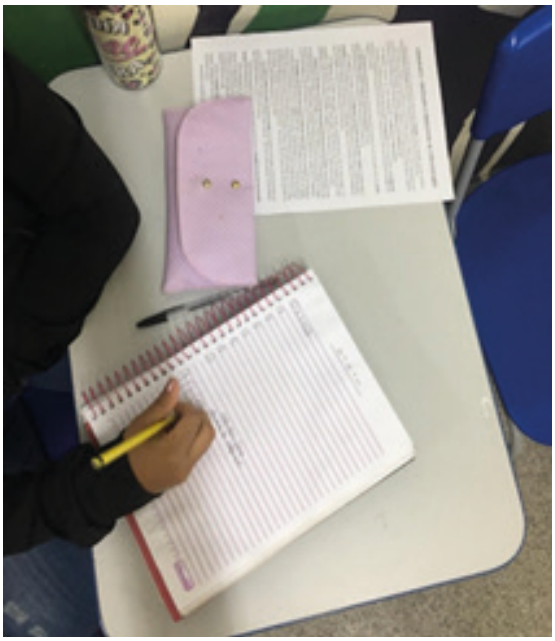
Nesta etapa da atividade, resgatou-se os procedimentos teóricos anteriormente mencionados para determinar a matriz inversa. Além disso, explicou-se que o procedimento realizado para a decodificação só foi possível porque a matriz C é inversível e, por este fato, ao multiplicar a matriz P por C^{-1}, pela esquerda, obtém-se a matriz M.

Em termos matemáticos, fez-se o seguinte:

$$C^{-1} \cdot P = C^{-1}(C \cdot M) = (C^{-1} \cdot C) \cdot M = I_2 \cdot M = M,$$

onde I_2 é a matriz identidade de *ordem 2*.

Figura 5. Alunos codificando e decodificando a mensagem.



Fonte: Acervo da pesquisa (2022).

Figura 6. Alunos resolvendo o desafio.

Fonte: Acervo da pesquisa (2022).

No último momento da oficina, foi proposto um desafio aos alunos com a colaboração do professor da turma. Solicitou-se ao docente que escolhesse uma palavra qualquer em segredo, esta seria criptografada por ele utilizando a mesma chave aleatória C dada anteriormente e, em seguida, decodificada pelos estudantes.

Após sanadas algumas dúvidas em relação à multiplicação de matrizes, os alunos conseguiram concluir o desafio com êxito obtendo a matriz da mensagem secreta, que, ao consultar o alfabeto, revelou-se que a palavra escolhida pelo professor foi a palavra NOTA.

RESULTADOS E DISCUSSÕES

Nesta seção, apresentam-se os dados do questionário avaliativo, disponibilizado via formulário *Google* aos alunos participantes da oficina. O questionário foi respondido por 37 (trinta e sete) discentes das 4 (quatro) turmas do 3º ano do Ensino Médio, onde a oficina foi executada e contava com as seguintes perguntas:

Pergunta 1: *Você compreendeu o que é criptografia?*
Pergunta 2: *A abordagem através da criptografia facilitou a compreensão sobre matrizes?*
Pergunta 3: *O que você achou da didática do ministrante da oficina?*
Pergunta 4: *O que você achou da oficina? Comente.*
Pergunta 5: *Qual parte da oficina você achou mais interessante?*

Do universo que responderam ao questionário avaliativo, 97,3% dos alunos informaram compreender o conceito de criptografia.

Cabe lembrar que, no início da oficina, antes de introduzir o conceito de criptografia, os alunos foram questionados se sabiam do que se tratava e somente a metade informou que tinha escutado sobre o assunto, mas que não sabia explicar o que significava.

Considerando a segunda pergunta, 94,6% dos alunos responderam que a abordagem por meio da criptografia facilitou a compreensão dos tópicos de matrizes abordados na oficina. Com esse resultado, pode-se inferir que o uso da criptologia, além de despertar a curiosidade dos estudantes, é uma potencialidade no processo de absorção do conhecimento sobre matrizes.

Observando o gráfico com as respostas da Pergunta 3, na Figura 7, constatou-se que a didática do ministrante da oficina foi bem avaliada pelos alunos, uma vez que 56,8% atribuíram o conceito ótimo e 43,2% o conceito bom.

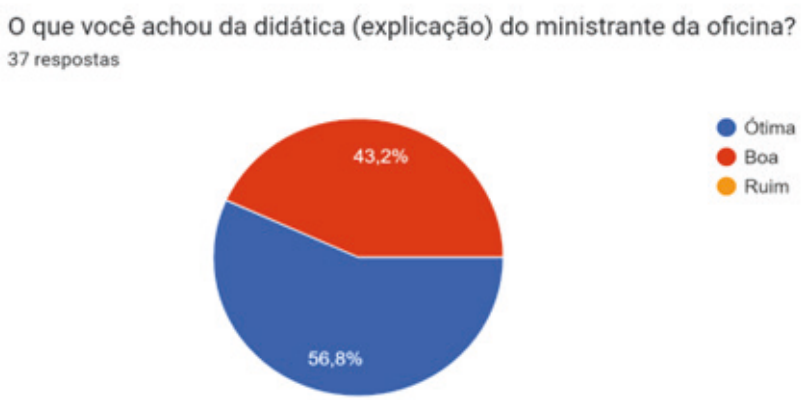
Estes dados também são corroborados por alguns comentários obtidos na Pergunta 4, conforme segue:

> *- Muito interessante, os temas abordados de forma geral, foi uma boa experiência, e o professor repassou o conteúdo de forma muito boa e que deu para entender bastante.*
> *- Achei bom, bem dinâmico, interação do professor foi boa para compreensão do assunto.*
> *- Ótima! Eu achei muito didática e divertida.*
> *- Super interessante, normalmente não participo de resoluções de trabalhos em sala, dessa vez me senti animada para realizar a atividade.*
> *- Interessante! O professor é prático e a explicação foi ótima, aprendi com facilidade.*

Analisando os comentários obtidos na Pergunta 4, conclui-se que a grande maioria dos alunos teve uma boa percepção do assunto matrizes mediante a aplicação da criptografia.

Assim, depreende-se a importância de que o professor utilize novas estratégias de ensino para capturar a atenção do aluno, com o intuito de que a aula seja mais produtiva e que os alunos possam aprender com mais facilidade e interesse, conforme se observa no relato acima: "superinteressante, normalmente não participo de resolução de trabalhos em sala, dessa vez me senti animada para realizar a atividade".

Figura 7. Gráfico sobre a didática do palestrante da oficina.



Fonte: Formulário preenchido pelos alunos da Escola Augusto Meira (2022).

Em relação à Pergunta 5, pode-se constatar que a parte mais interessante da oficina para os alunos foi o método empregado para a explanação do assunto, pois o ministrante

utilizou ferramentas capazes de aguçar a curiosidade e fazer com que os estudantes prestassem mais atenção, como, por exemplo, a utilização de filmes como referências para explicar o uso da criptografia e sua importância; os métodos criptográficos, entre eles, a cifra de Hill, utilizada no processo de codificação e decodificação das mensagens dadas no exemplo e no desafio. Esses mecanismos foram capazes de proporcionar aos discentes melhor aproveitamento e compreensão sobre o conteúdo abordado, como pode-se verificar nas seguintes respostas à Pergunta 5:

> *- Foi quando ele explicou tudo sobre matrizes de forma que todos interagiram com perguntas, e o professor deixou bem claro o assunto sobre matrizes, foi uma aula muito boa.*
> *- Quando ele usou filmes como exemplo para explicar sobre a criptografia e propôs um desafio para turma (eu ganhei) :).*
> *- As referências de filmes. O alfabeto posto em números.*
> *- A parte sobre criptografia e questões de como criar uma senha codificada.*
> *- Tudo, a abordagem dos conteúdos foi bem explicada e deu para entender bem.*
> *- O momento em que nos foi apresentada a leitura da criptografia (a tradução).*
> *- A dinâmica de decodificação de códigos.*

Portanto, os resultados da pesquisa foram importantes para a compreensão da necessidade do docente em buscar alternativas metodológicas que estimulem a participação discente no processo de ensino e aprendizagem de matrizes, utilizando exemplos que possam ser aplicados no cotidiano do aluno. A realização de aulas que desafiem a interação e a participação dos discentes é de suma importância para que eles possam aprender o que foi repassado em sala de aula e sejam motivados a sempre buscar conhecimento.

A criptografia está intimamente presente na vida das pessoas, muitas vezes de forma imperceptível, sendo assim é adequado utilizá-la como ferramenta motivadora para a aprendizagem da Matemática, despertando nos alunos o prazer em aprender, conhecer e realizar atividades relacionadas ao ensino.

As dificuldades apresentadas pelos alunos na aprendizagem da Matemática decorrem de vários fatores, entre eles pode-se destacar: "a falta de contextualização do conteúdo abordado e a procura por soluções para amenizar essa situação, o que demanda do professor de matemática comprometimento, criatividade, persistência, espírito inovador, entre outras virtudes" (GRISELI, 2018, p. 10).

Dessa forma, os dados da pesquisa contribuíram para se ter uma visão crítica da importância de adotar métodos diferenciados como a utilização da criptografia para complementar a abordagem tradicional do ensino de matrizes, possibilitando uma aula mais dinâmica e fazendo com que o discente tenha prazer de estar em sala e com interesse naquilo que o professor está ensinando.

CONSIDERAÇÕES FINAIS

Ao final deste trabalho, considera-se que o estudo da criptografia possibilita aos alunos uma interação com o conteúdo de matrizes de forma contextualizada, e que interliga os

temas matemáticos a um tema atual, de forma que se verifica a presença da criptografia em diferentes situações e aplicações reais do aluno.

A partir dos estudos e pesquisas feitos sobre criptografia e matrizes, apura-se a grande importância em analisar e estudar cada detalhe presente na história e desenvolvimento de ambos os temas, tendo como proposta trabalhar métodos criptográficos que se aliam a conceitos matemáticos, como na atividade realizada na oficina, cujos processos de codificação e decodificação se deram a partir de uma cifra bastante conhecida, chamada cifra de Hill, que por sua vez se alia a conteúdos matriciais.

Outros métodos criptográficos também foram estudados, como: a cifra de César, a cifra de Vigenère e as máquinas criadas no período da Segunda Guerras Mundial. Esses métodos vistos no decorrer do trabalho foram essenciais para entender a história da criptografia, desde os tempos antigos até sua modernização tecnológica, proporcionando, dessa maneira, uma viagem no tempo em relação ao histórico da criptografia.

Entende-se, portanto, que a criptografia deveria estar mais presente nos currículos educacionais do Ensino Médio, uma vez que seu uso se apresenta com muita aplicabilidade em diversas áreas importantes e interessantes, não apenas da Matemática como em várias outras ciências, como, por exemplo, na área computacional, que interliga segurança de dados, arquivos confidenciais, dados bancários e muitos outros, ou seja, a influência da criptografia nos dias passados e atuais é de extrema importância para humanidade, posto que está ligada à privacidade e à confiança do ser humano e de seus bens, tornando-se um dos vieses motivadores que despertam o interesse em aprender conteúdos matemáticos.

Por meio da oficina matemática realizada em sala de aula, pode-se perceber e conhecer a importância do planejamento docente. A atividade foi muito interessante e empolgante, observando o interesse dos alunos aliado à vontade e motivação em aprender através de uma aula diferente e dinâmica, na qual foi possível ter uma visão de quais métodos podem contribuir para o ensino e aprendizagem dos alunos.

Portanto, espera-se que este trabalho possa contribuir nas discussões e reflexões docentes em relação ao processo de ensino e aprendizagem de matrizes, proporcionando aos discentes a construção do conhecimento a partir da curiosidade em desvendar o mundo.

REFERÊNCIAS

ARINOS, E. J. S. **Criptografia**: aplicações no ensino fundamental e médio. 2014. 100f. Dissertação (Mestrado em Matemática) – Universidade Federal do Mato Grosso do Sul, Campo Grande, 2014.

BEZERRA, D. D. J.; MALAGUTTI, P. L.; RODRIGUES, V. C. D. S. Aprendendo criptologia de forma divertida. In: Bienal de Matemática, 5., 2010, João Pessoa, Paraíba. **Anais eletrônicos [...]**. Rio de Janeiro: SBM – Sociedade Brasileira de Matemática, 2010.

BRANDÃO, M. M. D. **Uma adaptação da Cifra de Hill para estudo de matrizes**. 2017. 92 f. Dissertação (Mestrado em Matemática) - Universidade Federal de Ouro Preto, Minas Gerais, 2017.

BRASIL. **Lei nº 9.394**, de 20 de desembro de 1996. Parâmetros Curriculares Nacionais (Ensino Médio). Brasília, 1996.

BRUNO. O. M. Criptografia: de arma de guerra a pilar da sociedade moderna. Artigo. **Jornal da USP**, 9 jan. 2017.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: IMPA, 2005.

DRUCK, S.; HELLMEISTER, C. P.; PEIXOTO, C. M. **Coleção Explorando o Ensino** – Matemática (Ensino Médio), v 3. Brasília: Ministério da Educação, Secretaria de Educação Básica, 2004.

GODOY, A. S. Introdução à pesquisa qualitativa e suas possibilidades. **Revista de administração de empresas**, v. 35, p. 57-63, 1995.

GRISELI, R. C. **Criptografia**: uma proposta para a educação básica. 2018. 106f. Dissertação (Mestrado em Matemática) – Universidade Federal da Fronteira Sul, Chapecó - SC, 2018.

MALAGUTTI, P. L. **Atividades de contagem a partir da criptografia**. Rio de Janeiro: IMPA, 2015. Disponível em: http://www.obmep.org.br/docs/apostila10.pdf. Acesso em: 05 set. 2022.

MOURA, M. D. O. **A criptografia motivando o estudo das funções no 9º ano do ensino fundamental**. 2019. 93f. Dissertação (Mestrado em Matemática) – Universidade Federal do Tocantins, Arraias, 2019.

REIS, F. D. Criptografia - Cifra de César. Artigo. **Revista Bóson - Treinamentos em Ciência e Tecnologia,** 2016.

REVISTA GALILEU. **Conheça a Pedra de Roseta, que mudou a história da arqueologia**. Artigo. 2021. https://revistagalileu.globo.com/Ciencia/Arqueologia/noticia/2018/07/conheca-pedra-de-roseta-que-mudou-historia-da-arqueologia.html.

ROSSETO, C. K. **Criptografia como recurso didático**: uma proposta metodológica aos professores de matemática. 2018. 84 f. Dissertação (Mestrado em Matemática) – Universidade Estadual Paulista, São Paulo, 2018.

TAMAROZZI, A. C. Codificando e decifrando mensagens. **Revista do Professor de Matemática**, v. 45, São Paulo: Sociedade Brasileira de Matemática, 2001. http://www.educadores.diaadia.pr.gov.br/arquivos/File/2010/veiculos_de_comunicacao/RPM/RPM45/RPM45_08.PDF

VIVIANI, D.; COSTA, A. et al. **Práticas de ensino de ciências biológicas**. Centro Universitário Leonardo da Vinci – Indaial, Grupo UNIASSELVI, 2010.

ZANCANELA, L. C. Proteção de dados. Artigo [on line] 2021. **Revista CRYPTOID**.

Histórico

Recebido: 25 de agosto de 2023.
Aceito: 10 de dezembro de 2023.
Publicado: 30 de dezembro de 2023.

Como citar – ABNT

FERREIRA, Sávio dos Reis; ARRUDA, Suellen Cristina Queiroz. A criptografia no ensino de matrizes na Educação Básica. **Revista de Matemática, Ensino e Cultura – REMATEC**, Belém/PA, n. 43, e2023034, 2023. https://doi.org/10.37084/REMATEC.1980-3141.2023.n43.pe2023034.id516

Como citar – APA

FERREIRA, S. R.; ARRUDA, S. C. Q. (2023). A criptografia no ensino de matrizes na Educação Básica. ***Revista de Matemática, Ensino e Cultura – REMATEC***, (43), e2023034. https://doi.org/10.37084/REMATEC.1980-3141.2023.n43.pe2023034.id516