UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Joaquim Denilson de Souza Silva

Produto de Hadamard, Criptografia e Suas Aplicações Didático-Conceituais no Ensino Básico

Campina Grande - PB
Agosto/2025

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Joaquim Denilson de Souza Silva

Produto de Hadamard, Criptografia e Suas Aplicações Didático-Conceituais no Ensino Básico

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Orientadores: Prof. Dr. Luiz Antônio da Silva Medeiros
Prof. Dr. José Lucas Galdino da Silva

Campina Grande - PB
Agosto/2025

S586p Silva, Joaquim Denilson de Souza.

Produto de Hadamard, criptografia e suas aplicações didático-conceituais no ensino básico / Joaquim Denilson de Souza Silva. – Campina Grande, 2025.

111 f. : il. color.

Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, 2025.

"Orientação: Prof. Dr. Luiz Antônio da Silva Medeiros, Prof. Dr. José Lucas Galdino da Silva".

Referências.

1. Produto de Hadamard. 2. Criptografia. 3. Ensino de Matemática. 4. Matemática Aplicada. I. Medeiros, Luiz Antônio da Silva. II. Silva, José Lucas Galdino da. III. Título.

CDU 51:37(043.3)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA MEIRE EMANUELA DA SILVA MELO CRB-15/568

Joaquim Denilson de Souza Silva

Produto de Hadamard, Criptografia e Suas Aplicações Didático-Conceituais no Ensino Básico

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Trabalho aprovado. Campina Grande - PB, 29 de agosto de 2025:

gov.br
Documento assinado digitalmente
LUIZ ANTONIO DA SILVA MEDEIROS
Data: 19/09/2025 16:59:13-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Luiz Antônio da Silva Medeiros
Orientador

Profa. Dra. Laise Dias Alves Araújo
Membro externo - UFERSA

Prof. Dr. Romildo Nascimento de Lima
Membro interno - UFCG

Campina Grande - PB
Agosto/2025

À minha mãe, cujo ventre me abrigou, cujo colo me acalmou, cujos ensinamentos me salvaram, salvarão meus filhos e os filhos deles.

Agradecimentos

A meu Senhor Jesus, que me sustentou nas dores que só Ele é capaz de compreender. Nesta maravilhosa e desafiadora jornada, o mundo tentou me derrubar de muitas maneiras, mas meu Deus me sustentou.

Aos meus pais, pelo carinho e cuidado ao longo de todo o caminho que me trouxe até aqui.

À minha tia Preta, pelo exemplo, apoio financeiro e por sempre acreditar em mim.

Ao professor Romildo, pela sua empatia e pela busca incansável por bolsas, que me proporcionaram segurança financeira nesta dispendiosa batalha. Nosso país precisa de mais servidores dedicados e exemplares como o senhor!

À Fundação de Apoio à Pesquisa do Estado da Paraíba – FAPESQ, e a todos os servidores que a compõem, pelo apoio financeiro e pelo incentivo à pesquisa, que possibilitaram a execução deste trabalho.

Aos meus orientadores, Prof. Dr. Luiz Antônio da Silva Medeiros e Prof. Dr. José Lucas Galdino da Silva, pela dedicação, paciência e pelas valiosas contribuições, fundamentais para a realização deste trabalho.

Aos colegas e amigos, pelo companheirismo, pelas trocas de experiências e pelo apoio ao longo da jornada acadêmica.

À Universidade Federal de Campina Grande – UFCG, pela oportunidade e pelo espaço de aprendizado e crescimento.

A todos que, de alguma forma, contribuíram para a concretização deste trabalho, deixo registrado meu sincero agradecimento.

O Senhor te guardará de todo o mal;
guardará a tua alma.
O Senhor guardará a tua entrada e a tua saída,
desde agora e para sempre.
(Bíblia Sagrada, Salmo 121:7-8)

Resumo

Este trabalho investiga o Produto de Hadamard, suas propriedades e características, propondo-o como recurso pedagógico para o ensino de conceitos matemáticos e criptográficos na educação básica. Inicialmente, realiza-se uma análise bibliográfica mista, de caráter quantitativo e qualitativo, que evidencia a predominância da aritmética modular e do sistema RSA na produção acadêmica nacional sobre criptografia, especialmente no contexto do PROFMAT. Paralelamente, constata-se a ausência do Produto de Hadamard como objeto de estudo na matemática escolar e em trabalhos brasileiros. A pesquisa internacional confirma que, embora essa operação seja mencionada em contextos avançados, raramente é associada ao Ensino Básico. Diante desse cenário, foi desenvolvido um Produto Educacional composto por uma sequência didática que aborda fundamentos históricos da criptografia, cifras clássicas e aplicações do Produto de Hadamard em sistemas de criptografia de imagens, com foco em seu potencial como ferramenta de motivação e contextualização da Matemática. A proposta fundamenta-se na Educação Matemática Realística, na Modelagem Matemática e nas competências previstas pela BNCC, buscando promover uma aprendizagem mais significativa e aproximar os estudantes de contextos contemporâneos em que a criptografia se insere.

Palavras-chave: Produto de Hadamard; Criptografia; Ensino de Matemática.

Abstract

This study investigates the Hadamard Product, its properties and characteristics, proposing it as a pedagogical resource for teaching mathematical and cryptographic concepts in basic education. Initially, a mixed bibliographic analysis — both quantitative and qualitative — is conducted, revealing the predominance of modular arithmetic and the RSA system in national academic production on cryptography, especially within the PROFMAT context. At the same time, the absence of the Hadamard Product as a subject of study in school mathematics and Brazilian research is noted. International studies confirm that although this operation is mentioned in advanced contexts, it is rarely associated with basic education. Based on this scenario, an Educational Product was developed consisting of a didactic sequence that addresses historical foundations of cryptography, classical ciphers, and applications of the Hadamard Product in image encryption systems, focusing on its potential as a tool for motivation and contextualization in mathematics. The proposal is grounded in Realistic Mathematics Education, Mathematical Modeling, and the competencies established by the BNCC, aiming to foster more meaningful learning and connect students with contemporary contexts in which cryptography is embedded.

Keywords: Hadamard Product; Cryptography; Mathematics Education.

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

Este trabalho tem como foco o Produto de Hadamard e suas aplicações em criptografia. O tema se destaca pela simplicidade de sua definição em contraste com suas aplicações significativas no estudo das matrizes e na criptografia. As matrizes desempenham um papel fundamental no Ensino Básico, especialmente na segunda série do Ensino Médio, segundo a Secretaria de Estado da Educação da Paraíba (2023), os objetivos de aprendizagem da unidade temática Álgebra incluem: (i) "identificar e representar os diferentes tipos de matrizes" e (ii) "resolver problemas utilizando as operações com matrizes e a linguagem matricial". No contexto do segundo objetivo, ao abordar operações com matrizes, muitos estudantes demonstram dificuldades ao compreender o produto usual de matrizes. Esse fator motivou nosso interesse pelo Produto de Hadamard, cuja multiplicação matricial mais intuitiva, conforme observamos em nossa prática em sala de aula, pode servir como um elemento motivador no ensino.

No mesmo sentido, segundo Base Nacional Comum Curricular (2018), sua quinta competência geral envolve as seguintes capacidades:

> Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva. (Base Nacional Comum Curricular, 2018, p. 9)

Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE) (2024), "a proporção de pessoas com 10 anos ou mais de idade que utilizaram a internet no país passou de 87,2% em 2022 para 88,0% em 2023. Em 2016, eram 66,1%." A pesquisa também aponta que "o equipamento mais utilizado para acessar a Internet em 2023 foi o telefone móvel celular (98,8%)." Assim, em um país cada vez mais digital, é essencial que o aluno desenvolva a capacidade de utilizar as tecnologias disponíveis, tais como o celular e computadores, por exemplo. Entretanto, a quinta competência geral vai além disso: ele precisa não apenas utilizar, mas também compreender e até mesmo ser capaz de criar tecnologias. Essa habilidade é o que Glister (1997) chama de letramento digital, definido por ele como "a capacidade de entender e usar a informação em múltiplos formatos a partir de uma vasta gama de fontes, quando apresentada por meio de computadores". Compreender o funcionamento é fundamental para que o aluno desenvolva um olhar mais crítico e possa propor melhorias ou até mesmo novos sistemas. Essa linha de pensamento também é defendida por Cassiano, Góes e Neves (2019), que destacam:

> Políticas públicas de tecnologias digitais voltadas ao instrumentalismo são limitantes, não será produzindo conhecimento por meio da mão de obra voltada unicamente para o mercado que iremos engendrar autonomia, liberdade e uma leitura distinta de mundo. Também não é possível afirmar que serão as tecnologias digitais que por si só irão desenvolver os países. Segundo Rosa e Trevisan (2016, p. 730), inicialmente tudo isso perpassa pela implantação de uma "tecnologia digital de cunho social e não de acordo com os interesses econômicos simplesmente". Não sendo dessa forma, é o mesmo que dar margem para possíveis desvios deste foco e, por conseguinte, problemas surgirão devido ao mau uso destas tecnologias. (CASSIANO; GÓES; NEVES, 2019, p. 55)

O autor critica o uso de políticas públicas que tratam as tecnologias digitais apenas como ferramentas para capacitação profissional. Para ele, ensinar a "usar" tecnologia de forma meramente instrumental, aplicada a funções específicas, sem compreender seu funcionamento e impacto, limita o desenvolvimento mais amplo e autônomo do estudante. Isso restringe sua capacidade crítica e a criação de novas ideias.

Assim, decidimos estudar o Produto de Hadamard por enxergarmos nele um potencial de uso como um elo, conectando o estudo de matrizes aos princípios por trás dos sistemas de criptografia moderna, além de despertar o interesse por ser um sistema de multiplicação de matrizes mais simples. Ao trabalhar esse tema em sala de aula, o professor poderá apresentar ao aluno o real significado da palavra "criptografia", que aparece, por exemplo, na página de conversas do WhatsApp. Além disso, poderá incentivá-lo a ir além do papel de mero usuário da tecnologia, colocando-o em uma posição de protagonismo.

Este estudo se justifica, pois, conforme nossas pesquisas, a literatura disponível apresenta lacunas significativas na abordagem desse tema. No capítulo seguinte, detalharemos as dificuldades encontradas. No entanto, podemos adiantar que, até o momento, não identificamos produções matemáticas nacionais sobre o Produto de Hadamard, sobretudo no contexto educacional. Os poucos trabalhos disponíveis, como o de Doniak (2006), exploram o Produto de Hadamard como uma ferramenta de otimização em sistemas de transmissão. Entretanto, por se tratar de uma pesquisa no ramo da engenharia, os conceitos matemáticos não são abordados com profundidade, tendo foco na aplicação prática das propriedades do produto.

Além disso, ao direcionarmos nossas pesquisas para fontes internacionais, percebemos que há uma riqueza de materiais sobre o tema. No entanto, a maioria deles pertence a um nicho muito distante do Ensino Básico. Desse modo, nosso trabalho pretende não apenas trazer esse tema para a literatura brasileira, mas também apresentá-lo de forma acessível para professores e estudantes do Ensino Básico.

Um dos primeiros contatos que se pode ter com o Produto de Hadamard, e que serviu como elemento motivador desta pesquisa, ocorre por meio da programação em

Python. Nesse ambiente, o símbolo "*" representa a multiplicação de escalares, mas, quando aplicado a matrizes, não retorna o produto matricial usual, e sim o Produto de Hadamard. Para obter o produto usual de matrizes em Python, é necessário utilizar o operador "@". Isso sugere que o Produto de Hadamard pode ser considerado o operador nativo de multiplicação de matrizes em Python.

Após a identificação dessa operação, investigamos suas aplicações e identificamos sua relevância na criptografia. O artigo Falcón et al. (2023) apresenta um interessante sistema de criptografia baseado no Produto de Hadamard. Dessa forma, reconhecemos dois elementos com potencial aplicação no Ensino Médio: (i) um produto de matrizes mais intuitivo e (ii) um sistema de embaralhamento de informações como sua aplicação.

Além disso, dentro da construção do sistema de criptografia apresentado no artigo, surge outro conceito altamente palpável para o Ensino Básico: os quadrados latinos. Esses quadrados constituem o elemento central do jogo Sudoku. Trata-se de um sistema rico em possibilidades de materialização da Matemática.

1.1 Objetivos

1.1.1 Objetivo geral

Este trabalho tem como objetivo principal estudar o Produto de Hadamard, suas propriedades e aplicações, com ênfase especial em sua utilização em sistemas de criptografia. Busca-se engajar alunos do Ensino Médio no aprendizado da Matemática, demonstrando a aplicabilidade desse conceito em sistemas de criptografia digital e analógica.

1.1.2 Objetivos específicos

O objetivo geral será alcançado por meio dos seguintes objetivos específicos:

- Definir e exemplificar o Produto de Hadamard;
- Enunciar e demonstrar suas propriedades fundamentais, tais como comutatividade, associatividade, inversibilidade e distributividade;
- Introduzir conceitos essenciais de sistemas de criptografia;
- Explorar um sistema de criptografia baseado no Produto de Hadamard;
- Desenvolver e analisar um produto educacional que auxilie no ensino e motive estudantes a se aprofundarem em conceitos matemáticos.

1.1.3 Metodologia

O tipo de pesquisa que melhor se encaixa na definição deste trabalho é a pesquisa bibliográfica exploratória. Segundo Theodorson (1969), essa abordagem pode ser definida da seguinte maneira:

> Estudo exploratório. Um estudo preliminar cujo propósito principal é se familiarizar com um fenômeno que deve ser investigado, para que o estudo principal a seguir possa ser projetado com maior compreensão e precisão. O estudo exploratório (que pode usar qualquer uma de uma variedade de técnicas, geralmente com uma pequena amostra) permite que o investigador defina seu problema de pesquisa e formule sua hipótese com mais precisão. Ele também o capacita a escolher as técnicas mais adequadas para sua pesquisa e decidir sobre as questões que mais precisam de ênfase e investigação detalhada, e pode alertá-lo sobre potenciais dificuldades, sensibilidades e áreas de resistência. (THEODORSON, 1969)

Para desenvolver este trabalho, realizamos uma ampla investigação sobre os estudos existentes, selecionamos aqueles mais adequados aos nossos propósitos e, a partir dessa base, aprofundamos nossa compreensão e refinamos a precisão dos temas explorados. A estrutura final foi reorganizada em uma narrativa coesa. Além disso, este trabalho contribui para a literatura acadêmica ao processar e estruturar conhecimentos provenientes de diversos estudos internacionais, propondo sua aplicação no Ensino Básico e divulgando o tema, ainda pouco explorado no contexto educacional brasileiro.

1.2 Organização

Decidimos organizar nosso trabalho em cinco capítulos, distribuídos da seguinte forma:

Capítulo 1 – Introdução: apresentamos o escopo do trabalho, sua motivação e relevância, além dos objetivos pretendidos.

Capítulo 2 – Análise Bibliográfica: expomos o referencial teórico que fundamenta nosso estudo. Para isso, utilizamos artigos acadêmicos encontrados no Google Acadêmico, dissertações do Profmat, publicações da Elsevier e documentos oficiais brasileiros que orientam e regulamentam a educação. Também detalhamos as fontes pesquisadas, os dados estatísticos relacionados aos trabalhos existentes e a metodologia adotada para nossas pesquisas.

Capítulo 3 – Fundamentação Teórica: abordamos toda a teoria Matemática necessária para a compreensão do objeto de estudo. Este capítulo contém definições, propriedades, teoremas e demonstrações essenciais ao desenvolvimento do trabalho.

Capítulo 4 – Criptografia: exploramos os tipos de ocultação da escrita, os sistemas criptográficos antigos e a forma como evoluíram ao longo dos anos. O capítulo

se encerra com a apresentação de um sistema criptográfico que utiliza o Produto de Hadamard em sua formulação.

Capítulo 5 – Aplicações Didáticas: apresentamos uma série de atividades que envolvem sistemas criptográficos antigos e o Produto de Hadamard aplicado à criptografia e ao comércio. Antes das atividades, expomos as bases metodológicas e a motivação para a escolha delas.

Capítulo 6 – Considerações Finais: apresentamos as conclusões obtidas a partir do estudo realizado. Destacamos as principais contribuições da pesquisa, analisamos as dificuldades encontradas ao longo do trabalho e sugerimos possíveis desdobramentos para estudos futuros. Além disso, refletimos sobre o impacto das aplicações abordadas no Ensino Básico, considerando suas implicações pedagógicas e a viabilidade de implementação em diferentes contextos educacionais.

2 Análise Bibliográfica

Neste capítulo, faremos uma abordagem detalhada de todos os aspectos presentes no processo de pesquisa para a elaboração deste trabalho. Diante dos elementos motivadores citados no capítulo anterior, iniciamos o levantamento bibliográfico das pesquisas já realizados na área. Essa fase do processo de produção de um estudo é extremamente importante, pois, segundo Sousa, Oliveira e Alves (2021, p. 65), a pesquisa bibliográfica:

> [...] nos auxilia desde o início, pois é feita com o intuito de identificar se já existe um trabalho científico sobre o assunto da pesquisa a ser realizada, colaborando na escolha do problema e de um método adequado, tudo isso é possível baseando-se nos trabalhos já publicados.(SOUSA; OLIVEIRA; ALVES, 2021, p. 65)

De fato, para assegurar a relevância e a consistência da produção científica, é necessário verificar o que a comunidade acadêmica já desenvolveu sobre o tema. Tal investigação nos ajudará a ter ciência dos problemas já conhecidos na área estudada, das soluções já encontradas, assim como dos pontos sobre os quais podemos contribuir. Isso se sustenta pelo que diz Macedo (1995), onde, para ele, a pesquisa bibliográfica deve tratar-se "[...] do primeiro passo em qualquer tipo de pesquisa científica, com o fim de revisar a literatura existente e não redundar o tema de estudo ou experimentação."(MACEDO, 1995, p. 13) Para o autor, essa não é apenas uma etapa importante, mas sim primordial. É indispensável que se faça uma "varredura" do que existe sobre o assunto, de modo a evitar a redundância e promover avanços reais no campo estudado.

2.1 Motivação

O Produto de Hadamard será introduzido formalmente no capítulo seguinte. No entanto, podemos antecipar que se trata de uma operação definida como a multiplicação de matrizes entrada a entrada — ou seja, elemento por elemento — de modo análogo à soma usual de matrizes, mas utilizando a multiplicação em vez da adição.

É provável que professores de Matemática, ao terem seu primeiro contato com o Produto de Hadamard, remetam-se às dificuldades enfrentadas por seus alunos durante o estudo de matrizes no Ensino Básico. A prática em sala de aula e os resultados de avaliações escolares indicam que os estudantes costumam compreender com maior facilidade a soma de matrizes do que a multiplicação usual entre elas.

Nesta seção, analisaremos um estudo que evidencia essa tendência: alunos, ao serem solicitados a realizar o produto usual de matrizes, frequentemente executam, de forma

intuitiva, o Produto de Hadamard, associando o procedimento à adição — ou seja, operando entrada por entrada.

O ensino tradicional de matrizes costuma iniciar-se com as operações de soma e subtração, que, por sua mecânica simples, costumam ser bem recebidas pelos alunos. A seguir, apresenta-se a multiplicação por escalar, que também é assimilada com facilidade, o que contribui para a construção de uma percepção positiva em relação ao conteúdo. No entanto, ao se introduzir a multiplicação usual de matrizes, muitos estudantes se deparam com um aumento significativo na complexidade da operação.

O estudo em questão foi realizado por Messias, Sá e Fonseca (2007), onde é feita uma análise das metodologias e dificuldades encontradas no ensino de matrizes na Educação Básica. Esta seção destrinchará os resultados obtidos e demonstrará como eles corroboram com a conclusão anteriormente mencionada.

Inicialmente, precisamos nos situar quanto à amostra da pesquisa citada. Segundo os próprios autores, a amostra da pesquisa:

> [...] contou com a participação de 109 universitários – 22 do 1º ano do curso de licenciatura em matemática da Universidade do Estado do Pará (UEPA) - 31 do 1º ano o curso de bacharelado em sistema de informação e 56 do 1º ano do curso de bacharelado em ciência da computação, ambos do Centro Universitário do Pará (CESUPA). A aplicação dos questionários foi realizada no período de 5 à 15 de Novembro de 2006.
>
> Optamos pelos alunos dos cursos citados acima devido ao fato deles terem estudado o assunto matrizes no ano anterior (3º ano do ensino médio) e porque o estudo de matrizes é muito importante para álgebra linear, disciplina estudada ao longo dos três cursos. (MESSIAS; SÁ; FONSECA, 2007, p. 2)

Assim, os dados apresentados a seguir referem-se a alunos aprovados em sistemas de seleção de universidades públicas, ou seja, aqueles que obtiveram melhores resultados nos vestibulares locais. Isso garante a boa qualidade da amostra. Ainda sobre a amostra, Messias, Sá e Fonseca (2007, p. 3) destaca que "a maioria dos alunos afirmou ter concluído o Ensino Médio em escola particular $(68,8\%)$", conforme pode ser visto na figura 1. [1] Com isso em mente, vejamos o teste aplicado.

[1] Nessa época, era comum as universidades públicas serem ocupadas majoritariamente por alunos provenientes da rede privada. Segundo Pessoa e Filho (2007, p. 32), "para o ano de 2005, 87,9% dos jovens matriculados no Ensino Médio brasileiro estavam em escolas públicas; somente 46,8% dentre eles ingressaram no ensino superior. Por outro lado, dos 12,1% de alunos matriculados em escolas particulares de Ensino Médio, 51,7% ingressaram no ensino superior público."

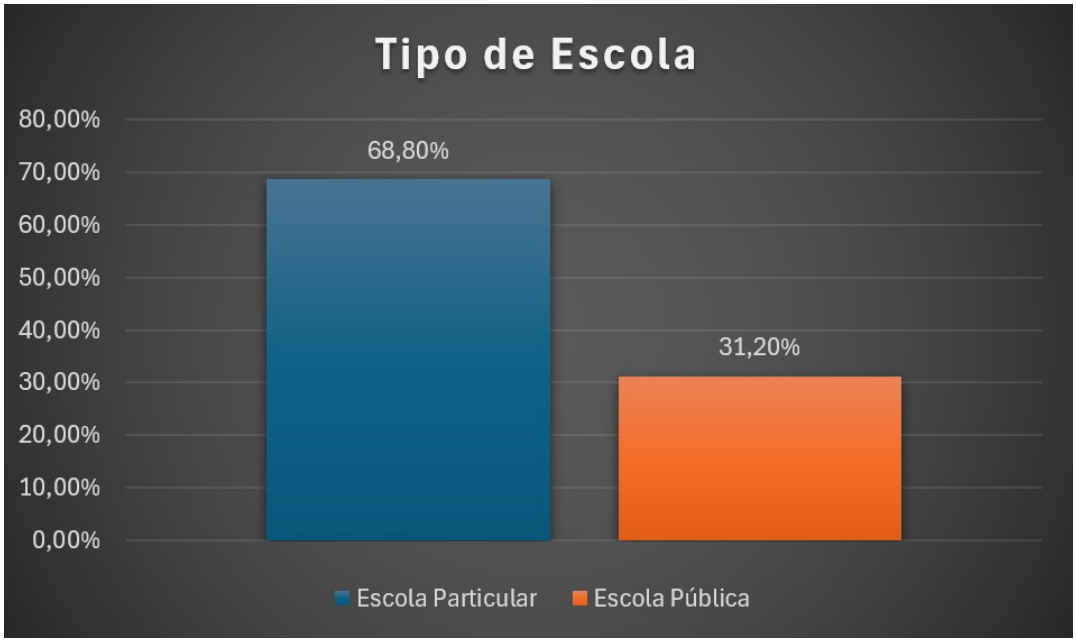


Figura 1 – Tipo de escola de origem da amostra (Gráfico elaborado pelo autor a partir de dados de Messias, Sá e Fonseca (2007).)

Fonte: (MESSIAS; SÁ; FONSECA, 2007)

Executando os protocolos elaborados para a pesquisa, os alunos fixaram as seguintes matrizes:

$$A = \begin{bmatrix} -8 & 0 \\ \frac{3}{5} & -\frac{2}{3} \end{bmatrix}, \quad B = \begin{bmatrix} -1 & -\frac{3}{5} \\ \frac{2}{3} & 6 \end{bmatrix}$$

Com isso, foi solicitado que encontrassem, entre as alternativas, qual representava corretamente a soma das matrizes, o produto e o determinante. As alternativas para a soma eram:

$$\text{a)} \begin{bmatrix} 8 & 0 \\ \frac{5}{8} & -4 \end{bmatrix} \quad \text{b)} \begin{bmatrix} -9 & -\frac{3}{5} \\ \frac{19}{15} & \frac{16}{3} \end{bmatrix} \quad \text{c)} \begin{bmatrix} -9 & \frac{3}{5} \\ \frac{1}{3} & \frac{4}{3} \end{bmatrix}$$

$$\text{d)} \begin{bmatrix} 9 & -\frac{3}{5} \\ \frac{16}{3} & \frac{19}{5} \end{bmatrix} \quad \text{e)} \begin{bmatrix} -8 & \frac{3}{5} \\ -\frac{2}{9} & \frac{19}{5} \end{bmatrix}$$

E os resultados obtidos são apresentados na Figura 2.

Os dados mostram que 79,81% assinalaram a alternativa correta. Conforme é concluído pelo próprio autor, a "maioria dos alunos não apresenta dificuldades quando se depara com itens relacionados à adição de matrizes." (MESSIAS; SÁ; FONSECA, 2007, p. 7)

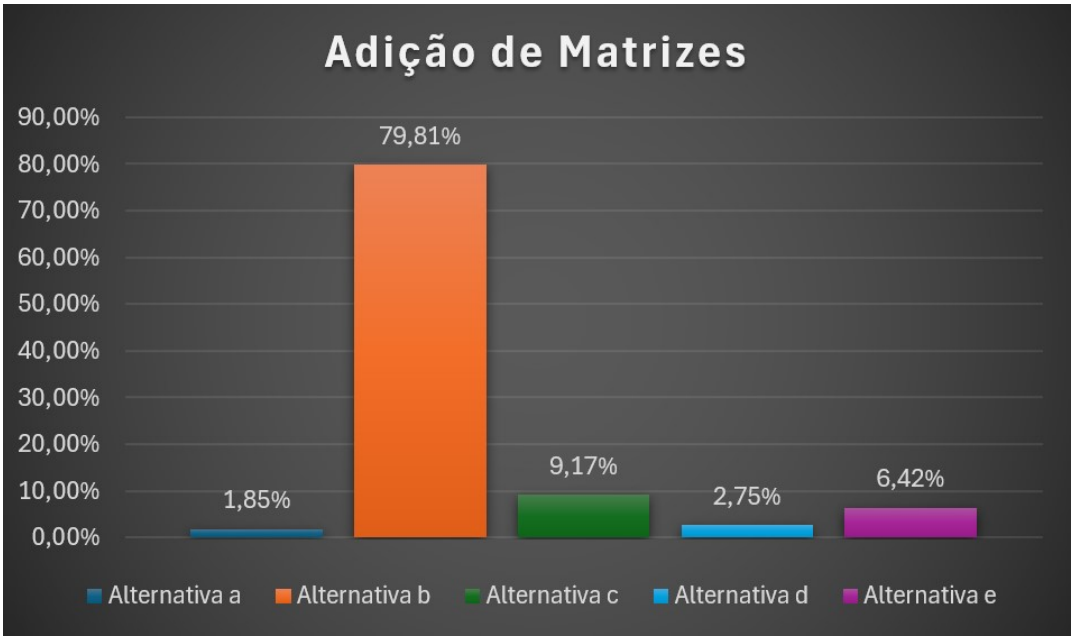


Figura 2 – Estatística de escolha para adição de matrizes (Gráfico elaborado pelo autor a partir de dados de Messias, Sá e Fonseca (2007).)

Fonte: (MESSIAS; SÁ; FONSECA, 2007)

Por outro lado, o mesmo não ocorre com o produto usual de matrizes. Para as mesmas matrizes A e B utilizadas anteriormente:

$$A = \begin{bmatrix} -8 & 0 \\ \frac{3}{5} & -\frac{2}{3} \end{bmatrix}, \quad B = \begin{bmatrix} -1 & -\frac{3}{5} \\ \frac{2}{3} & 6 \end{bmatrix}$$

foram fornecidas as seguintes alternativas como representação correta do produto usual dessas matrizes:

a) $\begin{bmatrix} -8 & 0 \\ \frac{2}{5} & -4 \end{bmatrix}$ b) $\begin{bmatrix} -8 & -\frac{9}{25} \\ -\frac{4}{9} & \frac{18}{5} \end{bmatrix}$ c) $\begin{bmatrix} -8 & -\frac{24}{5} \\ -\frac{47}{45} & -\frac{59}{25} \end{bmatrix}$

d) $\begin{bmatrix} 8 & \frac{24}{5} \\ -\frac{47}{45} & -\frac{109}{25} \end{bmatrix}$ e) $\begin{bmatrix} 8 & -\frac{4}{5} \\ -\frac{7}{45} & \frac{9}{25} \end{bmatrix}$

Ao observar a Figura 3, percebe-se que apenas 34,88% assinalaram a alternativa correta, enquanto 65,12% optaram por outras opções. Além disso, destaca-se um fato não enfatizado na pesquisa: a maioria dos alunos escolheu a alternativa “a”. Podemos concluir que, à exceção dos sinais, a matriz apresentada corresponde ao Produto de Hadamard entre as matrizes A e B.

Portanto, mesmo entre os primeiros colocados em um rigoroso sistema de seleção da região, ainda se observa uma significativa dificuldade na realização do produto usual de matrizes. Além disso, nota-se uma forte tendência dos alunos a aplicarem o Produto

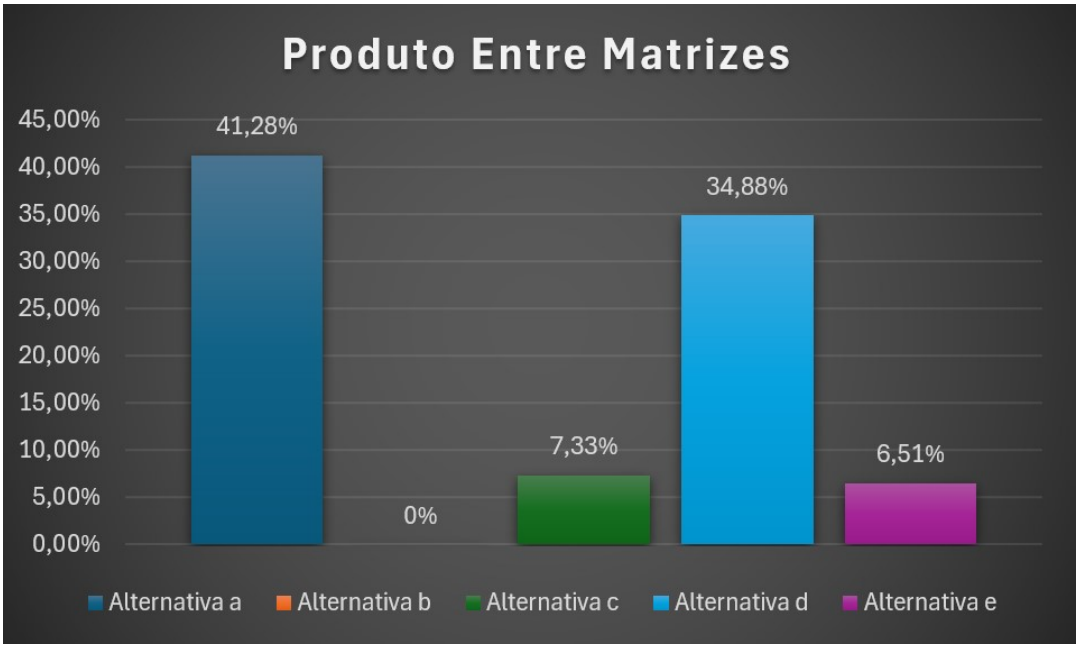


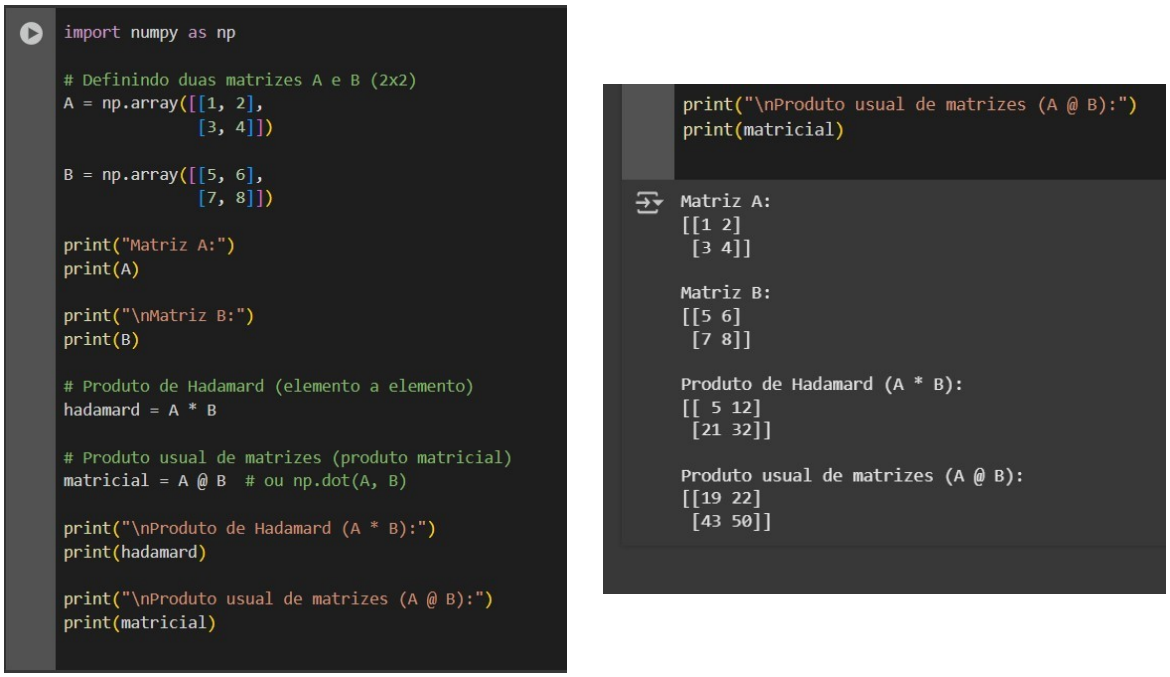
Figura 3 – Estatística de escolha para o produto de matrizes (Gráfico elaborado pelo autor a partir de dados de Messias, Sá e Fonseca (2007).)

Fonte: (MESSIAS; SÁ; FONSECA, 2007)

de Hadamard em vez do produto usual. Essa inclinação pode ser um ponto de partida promissor para abordar o Produto de Hadamard no Ensino Básico, evidenciando que, embora o produto de matrizes presente no componente curricular seja outro, e tenha fins distintos, aquele que os alunos acreditavam ser o procedimento correto também é uma operação formalmente definida e possui aplicações em áreas como criptografia de imagens, sistemas de recomendação de produtos, análise de valores de mercado, entre outras. Abordar esse tema contribui para enriquecer a cultura acadêmica dos estudantes.

Diversas aplicações do Produto de Hadamard estão diretamente associadas a sistemas computacionais. A título de exemplo, no sistema de criptografia que abordaremos mais adiante neste trabalho, formamos imagens a partir de grandes matrizes, nas quais cada elemento corresponde a um pixel. Realizar o produto usual entre matrizes desse tamanho demandaria um poder computacional muito maior do que o necessário com o Produto de Hadamard. Além disso, com o Produto de Hadamard, as cores dos pixels são embaralhadas, mantendo a nova cor na posição original do pixel e preservando, sobretudo, as dimensões das matrizes. O mesmo ocorre em sistemas de recomendação de produtos e na análise de valores de mercado, onde cada elemento da matriz possui um significado e sofre um produto que preserva sua posição. Ainda sobre suas aplicações, podemos citar sua forte presença na linguagem de programação. Na figura 4 podemos ver como o Python opera de forma nativa matrizes pelo Produto de Hadamard

enquanto um operador específico é usado para o produto usual.



```python
import numpy as np

# Definindo duas matrizes A e B (2x2)
A = np.array([[1, 2],
              [3, 4]])

B = np.array([[5, 6],
              [7, 8]])

print("Matriz A:")
print(A)

print("\nMatriz B:")
print(B)

# Produto de Hadamard (elemento a elemento)
hadamard = A * B

# Produto usual de matrizes (produto matricial)
matricial = A @ B  # ou np.dot(A, B)

print("\nProduto de Hadamard (A * B):")
print(hadamard)

print("\nProduto usual de matrizes (A @ B):")
print(matricial)
```

```
Matriz A:
[[1 2]
 [3 4]]

Matriz B:
[[5 6]
 [7 8]]

Produto de Hadamard (A * B):
[[ 5 12]
 [21 32]]

Produto usual de matrizes (A @ B):
[[19 22]
 [43 50]]
```

Figura 4 – Comparação entre o Produto de Hadamard e o produto matricial usual, ambos implementados em Python.

Fonte: Elaborado pelo autor (2025).

2.2 Análise bibliográfica mista

Nesta seção, abordaremos todos os aspectos envolvidos em nossa pesquisa bibliográfica. Faremos isso por meio da análise de quatro pontos: tipo de pesquisa, procedimentos de coleta de dados, procedimentos de análise de dados e justificativa das escolhas metodológicas.

2.2.1 Tipo de pesquisa

O método de pesquisa escolhido para realizar a análise bibliográfica foi o misto concomitante que, segundo (CRESWELL, 2010), são aqueles em que:

> [...] o pesquisador converge ou mistura dados quantitativos e qualitativos para realizar uma análise abrangente do problema da pesquisa. Nesse modelo, o investigador coleta as duas formas de dados ao mesmo tempo e depois integra as informações na interpretação dos resultados gerais. Além disso, nesse modelo, o pesquisador pode incorporar uma forma menor de dados com outra coleta de dados maior para analisar diferentes tipos de questões (o qualitativo é responsável pelo processo enquanto o quantitativo é responsável pelos resultados). Creswell (2010, p. 39)

Logo, uma pesquisa bibliográfica mista é aquela em que o pesquisador analisa a quantidade de trabalhos em um determinado escopo enquanto, de maneira concomitante, verifica a qualidade do que é trabalhado. Nossa pesquisa se enquadra neste método, pois, ao mesmo tempo em que fazemos a verificação do quantitativo de trabalhos com o tema desejado, analisamos também a forma como esses trabalhos abordam os temas propostos, a fim de reconhecer os caminhos de pesquisa comumente feitos ao se estudar criptografia e verificar possíveis lacunas a serem preenchidas.

Quantificar os trabalhos existentes e analisar a profundidade com que os temas são abordados permite não apenas compreender suas abordagens, mas também identificar quantos são, quais os mais recorrentes, em que contextos aparecem, além de outras informações relevantes. Um método puramente qualitativo não daria essa dimensão estatística da bibliografia, o que enfraqueceria a base da análise.

Ao adotar uma abordagem mista, nossa pesquisa ganha maior robustez analítica, pois a combinação entre dados quantitativos e qualitativos possibilita uma compreensão mais ampla e profunda da produção acadêmica sobre criptografia. O mapeamento quantitativo indica onde há maior ou menor concentração de estudos, enquanto a análise qualitativa revela como os temas são tratados. Isso nos permite direcionar com mais precisão nossas investigações, visando preencher lacunas deixadas pelos trabalhos já realizados.

2.3 Pesquisa nacional

Os elementos centrais buscados em trabalhos nacionais foram coletados do artigo de Falcón et al. (2023). Ele apresenta um método que usa quadrados latinos e o Produto de Hadamard para embaralhar números e posteriormente voltar à sua configuração original. Ou seja, um processo de criptografia eficiente. Associando esses números a pixels, podemos criptografar imagens. Com isso, identificamos como elementos-chave para nossa pesquisa: Produto de Hadamard, Criptografia e Matrizes.

Nossa investigação teve início com a análise de trabalhos realizados no programa do PROFMAT. Em Sociedade Brasileira de Matemática (2017), encontramos o catálogo de disciplinas do programa, no qual consta a disciplina MA14 – Aritmética. Essa disciplina aborda os conteúdos introdutórios necessários ao estudo do sistema de criptografia RSA,[2] além de introduzir diretamente esse sistema. Essa é provavelmente a influência que levou a produção de diversos trabalhos de criptografia com base em Aritmética e aplicação em RSA dentro do programa do PROFMAT, constatado em nossa pesquisa.

[2] RSA (Rivest–Shamir–Adleman)é um dos primeiros sistemas de criptografia de chave pública e é amplamente utilizado para a transmissão segura de dados.

Em 11 de novembro de 2024, realizamos uma busca pelo termo “criptografia” no repositório do PROFMAT e identificamos 121 trabalhos que o mencionam no título. Desses, 28 citam explicitamente a sigla RSA, representando aproximadamente 23% do total.

Coletamos uma amostra do grupo de trabalhos que citavam apenas criptografia no título, para análise dos conteúdos abordados. Analisamos sete trabalhos. Em apenas um deles, realizado em uma universidade do Mato Grosso, o conteúdo de matrizes foi abordado — e de forma bastante sutil —, associando letras do alfabeto a números, e realizando a encriptação por meio do produto usual da matriz mensagem com a matriz chave, criada pelo encriptador. O processo de desencriptação consistia na multiplicação da matriz cifrada pela inversa da matriz chave.

Outro trabalho, realizado na USP, desenvolve um rico estudo da história da criptografia, abordando seus tipos e marcas deixadas ao longo do tempo. Já os outros cinco se concentram basicamente em conceitos de aritmética modular e teoria dos números, aplicando-os em sistemas criptográficos como o RSA — um caminho que vem se consolidando como típico nesse campo de estudo.

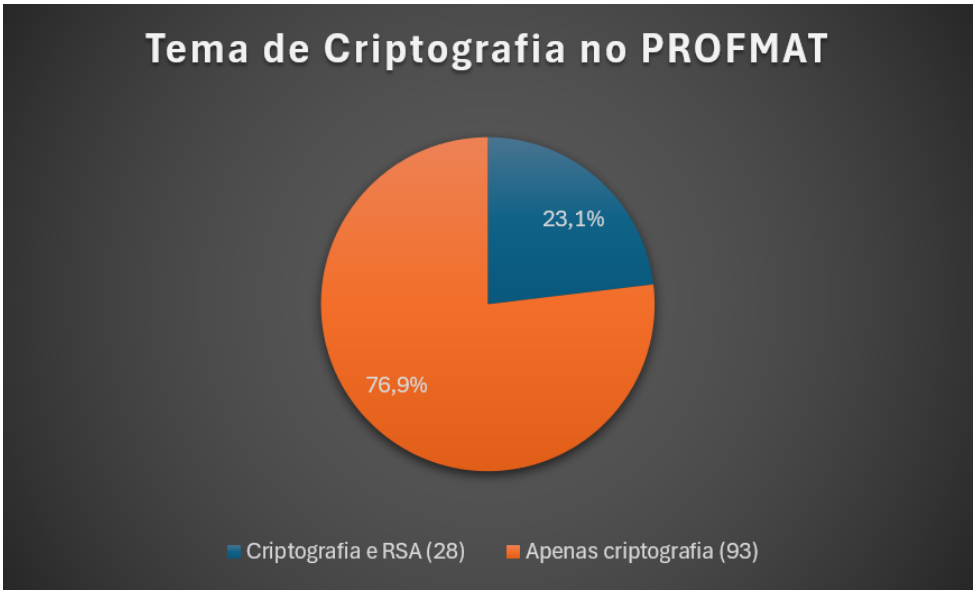


Figura 5 – Trabalhos do Repositório do Profmat com o termo Criptografia no título.

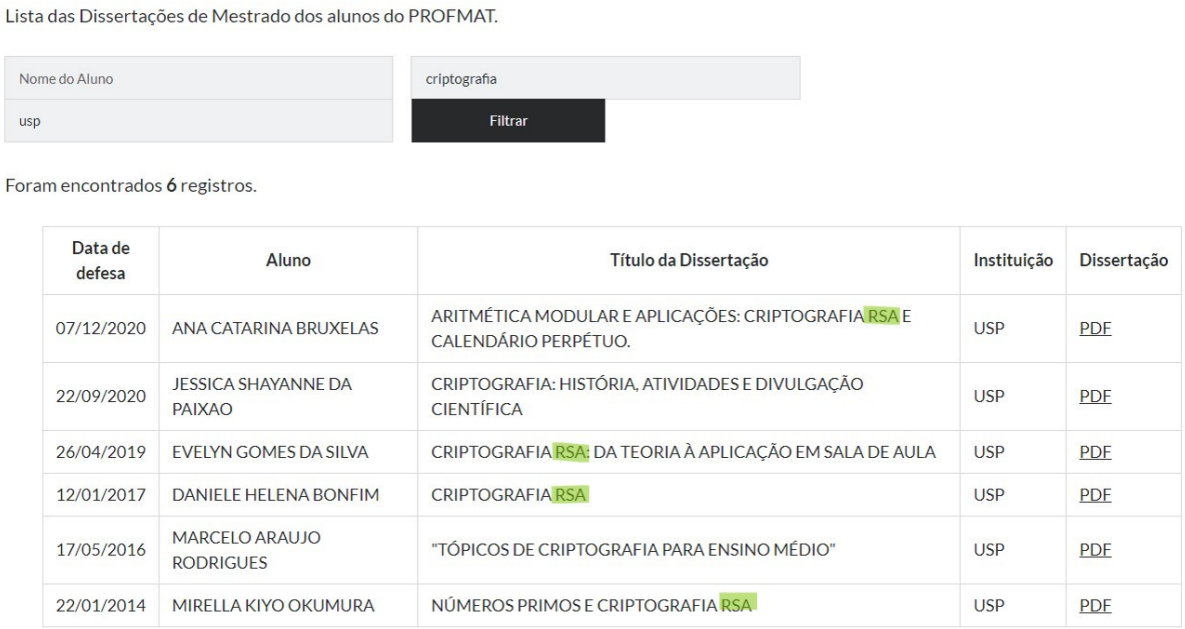
Fonte: Autoria própria.

Diante da quantidade expressiva de trabalhos relacionados à criptografia, decidimos afunilar ainda mais nossa pesquisa, concentrando-nos em dois grupos: a Universidade de São Paulo (USP) e universidades paraibanas (UFPB, UFCG e UEPB). A ecolha da USP se justifica pelo fato dela figurar, de maneira recorrente, como a melhor universidade do Brasil em diversos rankings nacionais e internacionais. De acordo com o Ranking Universitário Folha (RUF) 2024, por exemplo, a instituição lidera o ranking

geral pelo quarto ano consecutivo e ocupa a primeira colocação em 33 carreiras avaliadas (Folha de S. P., 2024). Já as universidades paraibanas, além de possuírem um alto padrão de qualidade, foram selecionadas para oferecer uma perspectiva sobre as temáticas em desenvolvimento na comunidade matemática local.

2.3.1 USP – Universidade de São Paulo

A Figura 6, retirada do repositório de dissertações do Profmat, mostra os resultados encontrados para os trabalhos realizados na USP onde a palavra "criptografia" aparecia no título.



Lista das Dissertações de Mestrado dos alunos do PROFMAT.

Nome do Aluno: usp

criptografia

Filtrar

Foram encontrados **6** registros.

Data de defesa	Aluno	Título da Dissertação	Instituição	Dissertação
07/12/2020	ANA CATARINA BRUXELAS	ARITMÉTICA MODULAR E APLICAÇÕES: CRIPTOGRAFIA RSA E CALENDÁRIO PERPÉTUO.	USP	PDF
22/09/2020	JESSICA SHAYANNE DA PAIXAO	CRIPTOGRAFIA: HISTÓRIA, ATIVIDADES E DIVULGAÇÃO CIENTÍFICA	USP	PDF
26/04/2019	EVELYN GOMES DA SILVA	CRIPTOGRAFIA RSA: DA TEORIA À APLICAÇÃO EM SALA DE AULA	USP	PDF
12/01/2017	DANIELE HELENA BONFIM	CRIPTOGRAFIA RSA	USP	PDF
17/05/2016	MARCELO ARAUJO RODRIGUES	"TÓPICOS DE CRIPTOGRAFIA PARA ENSINO MÉDIO"	USP	PDF
22/01/2014	MIRELLA KIYO OKUMURA	NÚMEROS PRIMOS E CRIPTOGRAFIA RSA	USP	PDF

Figura 6 – Dissertações do Profmat abordando criptografia na USP.

Fonte: Print de tela feito pelo autor a partir de pesquisa realizada no Sociedade Brasileira de Matemática (SBM) (2024) , em 11 nov. 2024.

Foram encontrados 6 trabalhos e, conforme destacado na Figura 6, 4 deles trazem a sigla "RSA" no próprio título, indicando que esse é um elemento central de estudo.

2.3.2 Universidades paraibanas

A Paraíba possui três polos do Profmat: um em João Pessoa, na Universidade Federal da Paraíba (UFPB), e outros dois em Campina Grande, sendo um na Universidade Federal de Campina Grande (UFCG) e o outro na Universidade Estadual da Paraíba (UEPB). No campo "Sigla da instituição" digitamos "PB" e em "Título da dissertação"

digitamos “criptografia”, resultando nos trabalhos da UFPB e da UEPB. Conforme se verifica na Figura 7, foram encontrados 6 trabalhos com a palavra “criptografia” no tema, restritos à Paraíba: 4 deles na UFPB e 2 na UEPB. Para a UFCG, cuja sigla não possui as letras “PB”, realizamos uma pesquisa isolada, que não retornou nenhum resultado.

Data de defesa	Aluno	Título da Dissertação	Instituição	Dissertação
27/02/2023	WÉLISSON MARTINS MOTA	TEORIA DOS NÚMEROS E CRIPTOGRAFIA RSA	UFPB	PDF
26/08/2016	JOSEMBERG DOS SANTOS SILVA	ALGUNS MÉTODOS DE CRIPTOGRAFIA	UEPB	PDF
26/09/2014	UELDER ALVES GALDINO	TEORIA DOS NÚMEROS E CRIPTOGRAFIA COM APLICAÇÕES BÁSICAS	UEPB	PDF
13/08/2013	ROBERVAL DA COSTA LIMA	CRIPTOGRAFIA RSA E A TEORIA DOS NÚMEROS	UFPB	PDF
13/08/2013	GLAUBER DANTAS MORAIS	A MATEMÁTICA VIA ALGORITMO DE CRIPTOGRAFIA ELGAMAL	UFPB	PDF
15/04/2013	THIAGO VALENTIM MARQUES	CRIPTOGRAFIA: ABORDAGEM HISTÓRICA, PROTOCOLO DIFFIE-HELLMAN E APLICAÇÕES EM SALA DE AULA	UFPB	PDF

Figura 7 – Dissertações do Profmat abordando criptografia nas universidades paraibanas.

Fonte: Print de tela feito pelo autor a partir de pesquisa realizada no Sociedade Brasileira de Matemática (SBM) (2024) , em 11 nov. 2024.

2.3.3 Produto de Hadamard nos trabalhos nacionais

Note que, nenhum dos trabalhos encontrados trata do Produto de Hadamard no título. Entretanto, a ausência vai além disso, ao verificar mais profundamente os trabalhos das Figuras 6 e 7 não encontramos menção ao Produto de Hadamard em momento algum dentro dos textos. Assim, percebemos que esse termo era mais restrito, o que nos levou a ampliar nossa pesquisa para todo e qualquer trabalho acadêmico no Brasil.

Buscamos o termo “Hadamard” em plataformas como o Banco de Dissertações da USP, Scielo e Google Acadêmico, sem encontrar nenhum trabalho na área de Matemática abordando o tema. Utilizamos, ainda, Inteligência Artificial (IA), especificamente o ChatGPT, que também foi incapaz de retornar algum trabalho brasileiro sobre o Produto de Hadamard na Matemática.

Os poucos trabalhos encontrados no Brasil pertenciam à área da engenharia, como a dissertação de mestrado em Engenharia Elétrica de Doniak (2006). Esse trabalho

aborda o funcionamento do OFDM (Orthogonal Frequency Division Multiplexing)[3]. Embora o Produto de Hadamard seja utilizado, ele não é explorado em profundidade, sendo mencionado apenas nas características relevantes para o OFDM.

2.4 Pesquisa Internacional

Com o objetivo de investigar trabalhos internacionais que abordam o Produto de Hadamard com foco em aplicações na educação básica ou em Matemática pura, foi realizado um levantamento bibliográfico em bases de dados acadêmicas amplamente reconhecidas. As etapas do procedimento estão descritas a seguir.

2.4.1 Google Scholar

Inicialmente, utilizou-se o Google Scholar para localizar artigos, dissertações e capítulos de livros relacionados ao tema. Foram aplicadas as seguintes expressões de busca:

- “Hadamard product” and “mathematics education”
- “Hadamard product” and “high school”
- “Hadamard product” and “pure mathematics”

Os resultado obtidos geralmente estavam ligados a conteúdos avançado de Matemática, como a Desigualdade de Oppenheim e Desigualdades na Álgebra de Spin de Jordan, conteúdos estudados apenas em pós-graduações específicas. Mesmo quando adicionado o termo “high school” o padrão persistia. Um dos estudos que fora capaz de fugir desse padrão foi o Barahmand (2020), onde é mostrado por que o produto usual de matrizes é definido da forma que conhecemos e quais critérios justificam essa escolha entre outras possibilidades de multiplicação. O Produto de Hadamard é citado, mas não é o foco do artigo. Ele serve como um exemplo de outra operação matricial legítima, que, embora útil em muitas aplicações, não satisfaz as mesmas propriedades que o produto padrão.

[3] Técnica de modulação que divide os bits em vários streams de taxa menor, para serem transmitidos por subcanais paralelos.

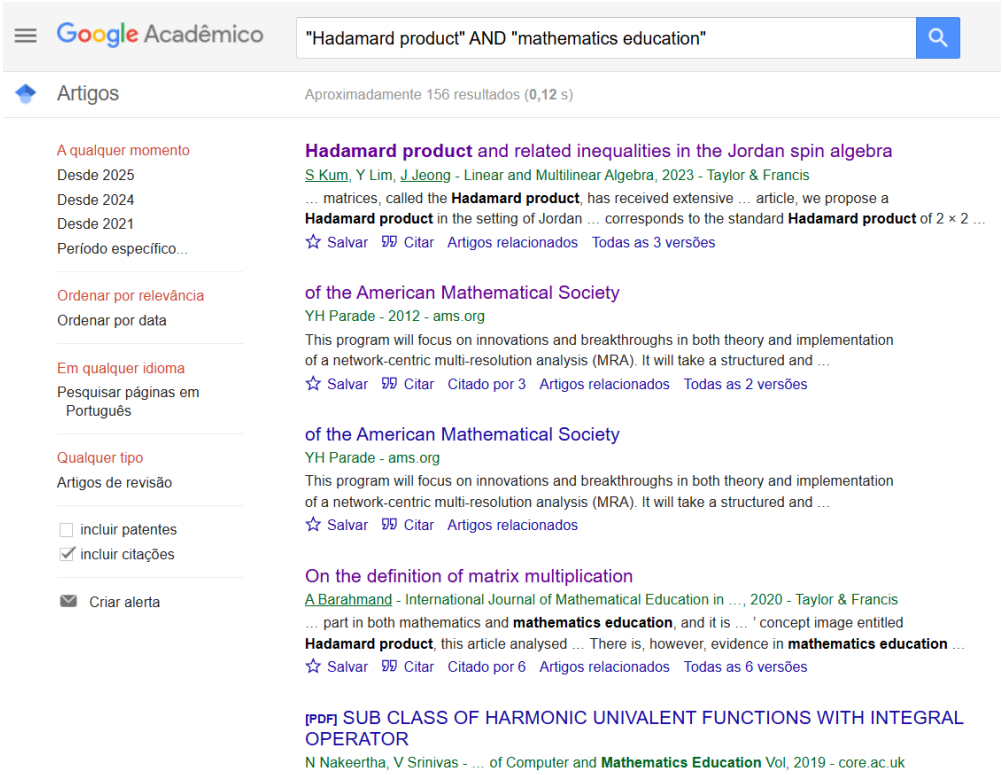


Figura 8 – Busca no Google Scholar com os termos “Hadamard product” e “mathematics education”.

Fonte: Print de tela feito pelo autor a partir de pesquisa realizada no Google Acadêmico (2025), em 4 jul. 2025.

2.4.2 Base ERIC

Também foi utilizada a base de dados ERIC, especializada em educação, aplicando o termo “Hadamard product” apenas um resultado foi retornado, o trabalho de Neudecker (1981). O texto trata do critério varimax de Kaiser, usado para interpretar fatores em análise fatorial. Mais uma vez trata-se de um trabalho distante do ensino básico, pois trata-se de um conteúdo típico de nível de pós-graduação em estatística.

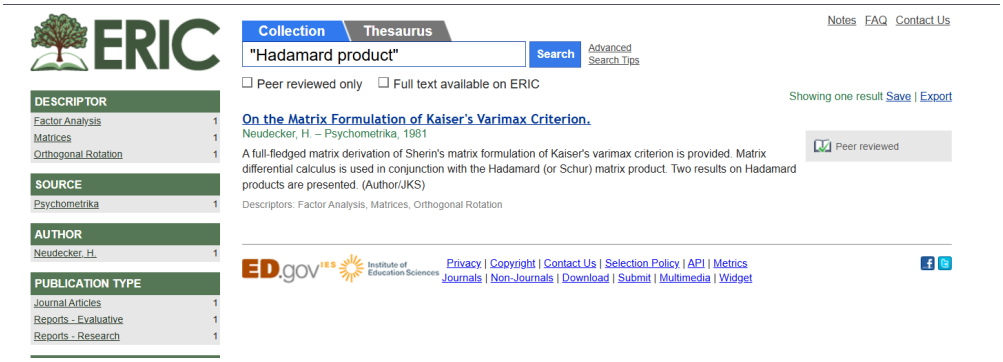


Figura 9 – Busca na base ERIC com os termos “Hadamard product”.

Fonte: Print de tela feito pelo autor a partir de pesquisa realizada na base ERIC – Education Resources Information Center (2025), em 4 jul. 2025.

2.5 Análise de dados das pequisas nacionais

Nossa análise revelou que o RSA é um elemento central quando se trata de criptografia. Mesmo os trabalhos que não abordam diretamente o RSA no título acabam tratando do tema. Por exemplo, Paixão (2020) apresenta um relato detalhado da história da criptografia e, na página 57, ao discutir a criptografia após a 2ª Guerra Mundial, menciona o RSA. Da mesma forma, Rodrigues (2016), no capítulo 5 (a partir da página 72), detalha o funcionamento e a construção do sistema RSA, apesar de seu trabalho ser voltado para o Ensino Médio.

Agora, observando de um ponto de vista macro o que foi feito nesses trabalhos, podemos notar que, tratando de fundamentação teórica, todos, sem exceção, se aprofundam na aritmética modular. Coisas como o Teorema de Fermat, a Função ϕ de Euler, o Teorema Chinês do Resto, por exemplo, são indispensáveis para trabalhos sobre o tema. Até mesmo Paixão (2020), que tem uma visão mais histórica, não consegue seguir um caminho diferente, pois a criptografia está profundamente enraizada na aritmética.

Sendo assim, o que podemos concluir ao analisar os trabalhos sobre criptografia da USP é que todos adentram a aritmética modular, assim como o RSA. Alguns abordam formas diversas de criptografia, até mesmo desligadas do mundo digital (como é o caso de Bonfim (2017)), mas o RSA permanece dominante.

Diferente do que encontramos na USP, aqui na Paraíba 2 dos 6 trabalhos contêm a sigla RSA no título. Entretanto, o mesmo padrão se repete com a abordagem do tema dentro dos trabalhos. Observamos que Silva (2016), no capítulo 4, aborda diversos tipos de criptografia, sendo um deles o RSA. O mesmo ocorre com Galdino (2014), mas agora no capítulo 6, sendo o RSA uma palavra-chave do trabalho. Já Morais

(2013) e Marques (2013) abordam o tema de forma bem mais discreta, com Marques (2013) citando o RSA como exemplo de criptografia assimétrica.

Diferente da USP, na Paraíba podemos perceber que os trabalhos realizados são mais antigos. Além disso, os 3 trabalhos de 2013 realizados na UFPB possuem o mesmo orientador, aparentando ser partes de uma pesquisa maior. Com isso, percebemos que o tema em nosso estado não foi tão explorado. Entretanto, assim como na USP, o RSA é extremamente presente.

A pesquisa nos trabalhos nacionais do PROFMAT revela uma forte tendência em desenvolver o conteúdo da disciplina Aritmética Modular. Ao tomar conhecimento dessa abordagem recorrente, percebemos que nosso trabalho poderia ser mais produtivo ao explorar aspectos diferentes da criptografia.

Sobre os caminhos a serem tomados, um trabalho que foi além do padrão encontrado, e que serviu de inspiração para esta produção, é a pesquisa de Paixão (2020). No capítulo 5, intitulado "Fundamentação Teórica", o autor faz o que a maioria dos demais também realizou: aborda os princípios matemáticos necessários para a compreensão dos sistemas criptográficos modernos. Tais princípios foram usados na formulação da fundamentação teórica, pois fornecem uma base sólida sobre o funcionamento dos sistemas criptográficos contemporâneos.

Entretanto, o apanhado histórico presente nos capítulos iniciais — baseado na obra de Singh (2001) — amplia a visão sobre a criptografia de maneira que poucos trabalhos fizeram. Analisar a história da criptografia oferece ao leitor uma perspectiva diferente dessa ciência, permitindo observar a eficácia de diversos sistemas que, embora não utilizassem a aritmética avançada dos métodos atuais, apresentavam algoritmos extremamente engenhosos e eficientes.

Consideramos que compreender o desenvolvimento histórico anterior aos sistemas modernos é fundamental para a construção significativa do aprendizado em criptografia.

2.6 Conclusões

Diante dos processos expostos neste capítulo, concluímos que o nosso trabalho poderá gerar um impacto relevante na área em que se propõe atuar, por abordar um tema praticamente inexistente na literatura nacional e que, mesmo em âmbito internacional, tem sido explorado de forma restrita, principalmente em contextos muito específicos da pós-graduação.

Acreditamos que o Produto de Hadamard, por ser um produto simples e de intuição natural para alunos do Ensino Médio, possa ser um conteúdo aderente ao aprendizado e uma porta de entrada para a introdução de sistemas mais avançados (como processos de encriptação digital), motivando e até direcionando a carreira desses estudantes.

Desse modo, defendemos sua utilização como recurso pedagógico no ensino de conceitos ligados à criptografia e à segurança da informação — temas que despertam o interesse dos jovens e dialogam com a realidade digital em que estão inseridos. Essa abordagem pode não apenas facilitar o acesso a conteúdos matemáticos mais abstratos, como também ampliar o horizonte dos estudantes em relação às aplicações da Matemática em áreas tecnológicas e científicas.

Portanto, ao propor essa articulação entre Matemática Elementar, Álgebra Matricial e temas de relevância tecnológica, o trabalho busca contribuir tanto para a inovação didática quanto para o fortalecimento da formação matemática na Educação Básica.

3 Fundamentação Teórica

Neste capítulo, definiremos formalmente o Produto de Hadamard estabelecendo algumas de suas propriedades mais interessantes, apresentando justificativas, demonstrações e exemplos. A literatura internacional dispõe de um vasto material sobre esse tema, abordando aspectos relevantes, porém, muitas vezes, com foco em conteúdos mais avançados. Um exemplo disso é o livro de Horn e Johnson (2012), que menciona propriedades discutidas neste capítulo, mas sem aprofundá-las. Nossa pesquisa insere-se no campo da Educação Matemática e, portanto, tem como principal interesse investigar as propriedades elementares do Produto de Hadamard, que servem como alicerce para um entendimento mais aprofundado desse conceito.

A base bibliográfica deste capítulo inclui os trabalhos de Million (2007) e Kishka et al. (2018), que apresentam de forma clara e detalhada as propriedades fundamentais desse produto. Realizamos aqui uma revisão da literatura com o objetivo de estabelecer as bases teóricas de nossa pesquisa, tornando este capítulo essencial para o desenvolvimento do trabalho. Além disso, complementamos as propriedades apresentadas e demonstradas com exemplos, buscando proporcionar ao leitor uma experiência mais intuitiva e facilitar a assimilação dos conceitos.

3.1 Produto de Hadamard

Estabelecemos as seguintes notações:

- $M_{m\times n}(\mathbb{R})$: O conjunto de matrizes de ordem $m \times n$ com entradas reais.
- $M_n(\mathbb{R})$: O conjunto das matrizes quadradas de ordem n com entradas reais.
- $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$, onde a_{ij} representa o elemento da linha i e da coluna j da matriz A.
- $\mathbb{N} = \{1, 2, 3, \dots\}$

Definição 3.1. *Dadas $A = [a_{ij}]$, $B = [b_{ij}] \in M_{m\times n}(\mathbb{R})$, definimos o Produto de Hadarmard entre A e B, denotado por $A \circ B$, como:*

$$A \circ B = [a_{ij} \cdot b_{ij}] \in M_{m\times n}(\mathbb{R})$$

Exemplo 1. Considere $A, B \in M_3(\mathbb{R})$, dadas por:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}, \quad B = \begin{bmatrix} 9 & 8 & 7 \\ 6 & 5 & 4 \\ 3 & 2 & 1 \end{bmatrix}.$$

Então, o produto de Hadamard de A por B é:

$$A \circ B = \begin{bmatrix} 1 \cdot 9 & 2 \cdot 8 & 3 \cdot 7 \\ 4 \cdot 6 & 5 \cdot 5 & 6 \cdot 4 \\ 7 \cdot 3 & 8 \cdot 2 & 9 \cdot 1 \end{bmatrix} = \begin{bmatrix} 9 & 16 & 21 \\ 24 & 25 & 24 \\ 21 & 16 & 9 \end{bmatrix}$$

Observação 1: O produto de Hadamard consiste de um produto ponto a ponto dos elementos correspondentes entre duas matrizes de mesma ordem.

Observação 2: Enquanto o produto usual de matrizes só é possível quando o número de colunas da primeira matriz seja igual ao número de linhas da segunda, no de Hadamard as matrizes devem apenas possuir as mesmas dimensões, ou seja, ter o mesmo número de linhas e colunas. Essa condição garante a boa definição do produto pois, assim sendo, cada elemento de uma matriz A terá um correspondente na matriz B para ser multiplicado.

Teorema 3.1. ***(Comutatividade:)*** *Dadas* $A = [a_{ij}]$, $B = [b_{ij}] \in M_{m\times n}(\mathbb{R})$. *Então* $A \circ B = B \circ A$.

Demonstração. A demonstração é resultado da propriedade de comutação dos reais, entrada das matrizes. Com efeito, sejam $A = [a_{ij}]$ e $B = [b_{ij}]$ matrizes de ordem $m \times n$ com entradas em $\mathbb{R}$. Partindo da Definição 3.1 temos:

$$A \circ B \overset{3.1}{=} [a_{ij} \cdot b_{ij}] \overset{1}{=} [b_{ij} \cdot a_{ij}] \overset{3.1}{=} B \circ A,$$

para todo $1 \leq i \leq m$ e $1 \leq j \leq n$. Onde (1) justifica-se por ser $[a_{ij}] \cdot [b_{ij}]$ produto usual de números reais.
Portanto, fica demonstrado que $A \circ B = B \circ A$. ■

Devemos nos lembrar que a multiplicação usual de matrizes possui um elemento neutro, a saber, a matriz identidade, denotada por I_n. A matriz identidade de ordem n é definida como:

$$I_n = \delta_{ij} = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}, \tag{3.1}$$

onde δ_{ij} denota-se por Delta de Kronecker.

O Produto de Hadamard também admite um elemento neutro, ou unidade, que é a matriz identidade para essa operação. Essa matriz é denotada por J_{mn} e consiste em uma matriz de ordem $m \times n$ cujos elementos são todos iguais a 1. Utiliza-se a letra J em vez de I para evitar confusão com a matriz identidade do produto usual de matrizes, preservando a distinção entre os dois tipos de operação.

Agora, mostraremos que no Produto de Hadamard vale a distributividade em relação a adição.

Teorema 3.2. ***(Associatividade):*** *Dadas as matrizes* $A = [a_{ij}]$, $B = [b_{ij}]$, $C = [c_{ij}] \in M_{m\times n}(\mathbb{R})$, *então* $A \circ (B \circ C) = (A \circ B) \circ C$.

Demonstração. Para qualquer i, j, temos:

$$A \circ (B \circ C) = [a_{ij}] \cdot (B \circ C) = [a_{ij}] \cdot [b_{ij}] \cdot [c_{ij}].$$

Além de que:

$$(A \circ B) \circ C = (A \circ B) \cdot [c_{ij}] = [a_{ij}] \cdot [b_{ij}] \cdot [c_{ij}].$$

Como ambos os lados resultam em $[a_{ij}] \cdot [b_{ij}] \cdot [c_{ij}]$, a propriedade é confirmada.

■

Exemplo 2. Se $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$ e $C = \begin{bmatrix} 9 & 10 \\ 11 & 12 \end{bmatrix}$, temos:

$$B \circ C = \begin{bmatrix} 5 \cdot 9 & 6 \cdot 10 \\ 7 \cdot 11 & 8 \cdot 12 \end{bmatrix} = \begin{bmatrix} 45 & 60 \\ 77 & 96 \end{bmatrix},$$

$$A \circ (B \circ C) = \begin{bmatrix} 1 \cdot 45 & 2 \cdot 60 \\ 3 \cdot 77 & 4 \cdot 96 \end{bmatrix} = \begin{bmatrix} 45 & 120 \\ 231 & 384 \end{bmatrix}.$$

$$(A \circ B) = \begin{bmatrix} 1 \cdot 5 & 2 \cdot 6 \\ 3 \cdot 7 & 4 \cdot 8 \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 21 & 32 \end{bmatrix}, \quad (A \circ B) \circ C = \begin{bmatrix} 5 \cdot 9 & 12 \cdot 10 \\ 21 \cdot 11 & 32 \cdot 12 \end{bmatrix} = \begin{bmatrix} 45 & 120 \\ 231 & 384 \end{bmatrix}.$$

Teorema 3.3. ***(Distributividade em relação a adição):***

Dadas as matrizes $A = [a_{ij}]$, $B = [b_{ij}]$, $C = [c_{ij}] \in M_{m\times n}(\mathbb{R})$, *então* $C \circ (A + B) = (C \circ A) + (C \circ B)$.

Demonstração. Temos que,

$$C \circ (A + B) = [c_{ij}] \cdot ([a_{ij}] + [b_{ij}]), \tag{3.2}$$

com isso, resumimos o Produto de Hadamar entre soma de matrizes em produto usual entre soma de elementos de matrizes, que por sua vez são números reais. Assim, podemos simplesmente aplicar a distributividade real, onde:

$$\begin{aligned} [c_{ij}] \cdot ([a_{ij}] + [b_{ij}]) &= [c_{ij}] \cdot [a_{ij}] + [c_{ij}] \cdot [b_{ij}] \\ &\overset{3.1}{=} (C \circ A) + (C \circ B). \end{aligned} \tag{3.3}$$

Portanto, $C \circ (A + B) = C \circ A + C \circ B$ para quaisquer matrizes A, B e C em $M_{m\times n}(\mathbb{R})$.

■

Exemplo 3. Se $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$ e $C = \begin{bmatrix} 9 & 10 \\ 11 & 12 \end{bmatrix}$, então:

$$B + C = \begin{bmatrix} 14 & 16 \\ 18 & 20 \end{bmatrix}, \quad A \circ (B + C) = \begin{bmatrix} 1 \cdot 14 & 2 \cdot 16 \\ 3 \cdot 18 & 4 \cdot 20 \end{bmatrix} = \begin{bmatrix} 14 & 32 \\ 54 & 80 \end{bmatrix}.$$

$$A \circ B = \begin{bmatrix} 5 & 12 \\ 21 & 32 \end{bmatrix}, \quad A \circ C = \begin{bmatrix} 9 & 20 \\ 33 & 48 \end{bmatrix}, \quad (A \circ B) + (A \circ C) = \begin{bmatrix} 14 & 32 \\ 54 & 80 \end{bmatrix}.$$

Teorema 3.4. ***(Distributividade e associatividade em relação ao produto por escalar):***

Seja $\alpha \in \mathbb{R}$ e $A = [a_{ij}]$, $B = [b_{ij}] \in M_{m\times n}(\mathbb{R})$. Então $\alpha \cdot (A \circ B) = (\alpha \cdot A) \circ B = A \circ (\alpha \cdot B)$.

Demonstração. Veja que:

$$\begin{aligned} \alpha \cdot (A \circ B) &= \alpha \cdot ([a_{ij}] \cdot [b_{ij}]) \\ &= \alpha \cdot [a_{ij}] \cdot [b_{ij}] \\ &\overset{(1)}{=} (\alpha \cdot [a_{ij}]) \cdot ([b_{ij}]) \\ &= ([\alpha \cdot a_{ij}]) \cdot ([b_{ij}]) \\ &\overset{3.1}{=} (\alpha \cdot A) \circ B. \end{aligned} \tag{3.4}$$

Isto prova a primeira equação. Analogamente:

$$\begin{aligned} \alpha \cdot [a_{ij}] \cdot [b_{ij}] &= [a_{ij}] \cdot \alpha \cdot [b_{ij}] \\ &\overset{(2)}{=} ([a_{ij}]) \cdot (\alpha \cdot [b_{ij}]) \\ &= ([a_{ij}]) \cdot ([\alpha \cdot b_{ij}]) \\ &\overset{3.1}{=} A \circ (\alpha \cdot B), \end{aligned} \tag{3.5}$$

onde (1) e (2) justificam-se pela propriedade associativa da multiplicação das entradas das matrizes que, em nosso caso, são números reais. Portanto, $\alpha \cdot (A \circ B) = (\alpha \cdot A) \circ B = A \circ (\alpha \cdot B)$ para quaisquer matrizes A e B em $M_{m\times n}(\mathbb{R})$ e $\alpha \in \mathbb{R}$.

■

Exemplo 4. Se $\alpha = 2$, $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$, então:

$$2(A \circ B) = \begin{bmatrix} 10 & 24 \\ 42 & 64 \end{bmatrix}, \quad (\alpha A) \circ B = \begin{bmatrix} 10 & 24 \\ 42 & 64 \end{bmatrix}.$$

Agora, dentro do universo do Produto de Hadamard, quais matrizes admitem inversa? O próximo teorema definirá a restrição de tais matrizes com sua devida demonstração.

Teorema 3.5. ***(Inversibilidade):***

Seja $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$. A terá uma inversa em Hadamard, denotada por $\hat{A}$, se e somente se, $a_{ij} \neq 0$ para todo $1 \leq i \leq m$ e $1 \leq j \leq n$, onde $\hat{A} = [\hat{a}_{ij}] = ([a_{ij}])^{-1}$. Além disso, vale que $A \circ \hat{A} = J$.

Demonstração. ($\Rightarrow$) Seja A uma matriz qualquer de em $M_{m\times n}(\mathbb{R})$ com inversa em Hadamard e seja Â tal inversa. O produto entre as inversas será a identidade, portanto, $A \circ \hat{A} = J_{mn}$. Em outras palavras, temos $[a_{ij}] \cdot [\hat{a}_{ij}] = 1$ para todo $1 \leq i \leq m$ e $1 \leq j \leq n$. Como a matriz A tem entradas reais podemos aplicar as propriedades de multiplicação usual em $\mathbb{R}$, de modo que: $[\hat{a}_{ij}] = (1)([a_{ij}])^{-1} = ([a_{ij}])^{-1}$, que só é possível quando todas as entradas de A forem invertíveis onde, nos reais, implica serem diferentes de zero. Portanto, $[a_{ij}] \neq 0$ para todo $1 \leq i \leq m$ e $1 \leq j \leq n$.

($\Leftarrow$) Por fim, seja A uma matriz qualquer em $M_{m\times n}(\mathbb{R} \setminus \{0\})$ para todo $1 \leq i \leq m$ e $1 \leq j \leq n$. Portanto, existem $([a_{ij}])^{-1}$ para todo i, j. Logo, por serem elementos de $\mathbb{R}$, temos $[a_{ij}] \cdot ([a_{ij}])^{-1} = 1 = ([a_{ij}])^{-1} \cdot [a_{ij}]$, o que prova ter A uma inversa Â definida por $[\hat{a}_{ij}] = ([a_{ij}])^{-1}$ para todo $1 \leq i \leq m$ e $1 \leq j \leq n$.

■

Logo, possuindo o Produto de Hadamard as propriedades de fechamento, associatividade, elemento neutro, comutatividade e elemento inverso, podemos concluir que as matrizes pertencentes ao conjunto $M_{m\times n}(\mathbb{R} \setminus \{0\})$ formam um Grupo Abeliano sobre o Produto de Hadamard.

Teorema 3.6. ***(Transposta):***

Dadas as matrizes $A = [a_{ij}]$, $B = [b_{ij}] \in M_{m\times n}(\mathbb{R})$, então $(A \circ B)^T = A^T \circ B^T$.

Demonstração. Por definição, se $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$, então $A^T = [a_{ji}] \in M_{n\times m}(\mathbb{R})$. Ou seja, a transposta de A é a matriz cujas linhas são as colunas de A.

Sejam $A = [a_{ij}]$ e $B = [b_{ij}]$, com $A, B \in M_{m\times n}(\mathbb{R})$. O Produto de Hadamard $A \circ B$ é definido como a matriz $[a_{ij} \cdot b_{ij}] \in M_{m\times n}(\mathbb{R})$, ou seja, cada elemento da matriz é obtido pela multiplicação dos elementos correspondentes de A e B na mesma posição.

Logo, aplicando a transposta ao Produto de Hadamard, temos:

$$(A \circ B)^T = [a_{ji} \cdot b_{ji}] \in M_{n\times m}(\mathbb{R}),$$

pois, ao transpor, as linhas tornam-se colunas, e os elementos da posição (i, j) da matriz original ocupam a posição (j, i) da transposta.

Por outro lado, ao calcular $A^T \circ B^T$, temos:

$$A^T = [a_{ji}] \in M_{n\times m}(\mathbb{R}),$$
$$B^T = [b_{ji}] \in M_{n\times m}(\mathbb{R}),$$
$$A^T \circ B^T = [a_{ji} \cdot b_{ji}] \in M_{n\times m}(\mathbb{R}).$$

Portanto, ambas as matrizes resultantes têm os mesmos elementos em todas as posições correspondentes. Assim, concluímos que:

$$(A \circ B)^T = A^T \circ B^T.$$

■

Exemplo 5. Se $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$, então:

$$(A \circ B)^T = \begin{bmatrix} 5 & 21 \\ 12 & 32 \end{bmatrix} = A^T \circ B^T.$$

Definição 3.2. *Dada uma matriz $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$ e um número natural $k \in \mathbb{N}$, definimos a potência de Hadamard (ou potenciação elemento a elemento) como:*

$$A^k = \underbrace{A \circ A \circ \cdots \circ A}_{k \text{ vezes}} = [a_{ij}^k]$$

Proposição 1: (Distributividade do Produto de Hadamard sobre Potenciação):

Dadas as matrizes $A = [a_{ij}]$, $B = [b_{ij}] \in M_{m\times n}(\mathbb{R})$ e um número natural $k \in \mathbb{N}$, tem-se:

$$[A \circ B]^k = [A]^k \circ [B]^k$$

Demonstração. Vejamos que:

$$\begin{aligned}
[A \circ B]^k &= \underbrace{(A \circ B) \circ (A \circ B) \circ \cdots \circ (A \circ B)}_{k \text{ vezes}} \\
&\overset{3.2}{=} \underbrace{(A \circ B \circ A \circ B \circ \cdots \circ A \circ B)}_{2k \text{ vezes}} \\
&\overset{3.1}{=} \underbrace{(A \circ A \circ \cdots \circ A)}_{k \text{ vezes}} \circ \underbrace{(B \circ B \circ \cdots \circ B)}_{k \text{ vezes}} \\
&= [A]^k \circ [B]^k,
\end{aligned}$$

desta forma:

$$[A \circ B]^k = [A]^k \circ [B]^k.$$

■

Proposição 2: (Potenciação de Potenciação): Dada uma matriz $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$ e um número natural $k \in \mathbb{N}$, tem-se:

$$\left([A]^k\right)^m = [A]^{k\cdot m}$$

Demonstração. Vejamos que:

$$\begin{aligned}
\left([A]^k\right)^m &= \underbrace{A^k \circ A^k \circ \cdots \circ A^k}_{m \text{ vezes}} \\
&= \underbrace{\overbrace{(A \circ A \circ \cdots \circ A)}^{k \text{ vezes}} \circ \overbrace{(A \circ A \circ \cdots \circ A)}^{k \text{ vezes}} \circ \cdots \circ \overbrace{(A \circ A \circ \cdots \circ A)}^{k \text{ vezes}}}_{m \text{ vezes}} \\
&\overset{3.2}{=} \underbrace{(A \circ A \circ \cdots \circ A)}_{m\cdot k \text{ vezes}} \\
&= [A]^{k\cdot m},
\end{aligned}$$

logo,

$$\left([A]^k\right)^m = [A]^{k\cdot m}.$$

■

Para a nossa próxima propriedade é importante primeiramente definirmos como se comporta uma matriz quando multiplicada por um escalar de maneira usual. Assim, dada uma matriz $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$ e $\alpha \in \mathbb{R}$ um escalar, define-se o produto da matriz A pelo escalar α como a matriz $\alpha{\cdot}A = [\alpha{\cdot}a_{ij}] \in M_{m\times n}(\mathbb{R})$, obtida multiplicando-se cada entrada de A pelo escalar α.

Em notação formal:

$$\alpha \cdot A = \alpha \cdot a_{ij}, \quad \text{para todo } 1 \leq i \leq m,\ 1 \leq j \leq n$$

Essa operação preserva a dimensão da matriz original e satisfaz as propriedades usuais da multiplicação escalar, como distributividade em relação à adição de matrizes e associatividade com a multiplicação de escalares.

Proposição 3: (Potenciação de produto por escalar): Seja $\alpha \in \mathbb{R}$ e $\alpha > 0$. Dada uma matriz $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$ e um número natural $k \in \mathbb{N}$, tem-se:

$$(\alpha \cdot [A])^k = \alpha^k \cdot ([A])^k.$$

Demonstração. Veja que:

$$\begin{aligned}(\alpha \cdot [A])^k &= [\alpha \cdot a_{ij}]^k \\ &= [(\alpha \cdot a_{ij})^k] \\ &= [\alpha^k \cdot a_{ij}^k] \\ &= \alpha^k \cdot [a_{ij}^k] \\ &= \alpha^k \cdot ([A])^k,\end{aligned}$$

consequentemente,

$$(\alpha \cdot [A])^k = \alpha^k \cdot ([A])^k.$$

■

Proposição 4: (Potência do Produto): Dada uma matriz $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$ e um número natural $k \in \mathbb{N}$, tem-se:

$$[A]^m \circ [A]^n = [A]^{m+n}$$

Demonstração. Claramente,

$$\begin{aligned}[A]^m \circ [A]^n &= (\underbrace{A \circ A \circ \cdots \circ A}_{m \text{ vezes}}) \circ (\underbrace{A \circ A \circ \cdots \circ A}_{n \text{ vezes}}) \\ &\overset{3.2}{=} \underbrace{(A \circ A \circ \cdots \circ A)}_{m+n \text{ vezes}} \\ &= [A]^{m+n},\end{aligned}$$

sendo assim,

$$[A]^m \circ [A]^n = [A]^{m+n}.$$

■

3.2 Aplicações

Segundo He et al. (2017), o Produto de Hadamard tem papel fundamental na construção de redes neurais voltadas para sistemas de recomendação personalizada. O autor aponta que camadas dessas redes são construídas com multiplicações elemento a elemento de vetores — ou seja, com o produto de Hadamard. Tais sistemas de recomendação são utilizados no comércio eletrônico; empresas como Amazon, Magazine Luiza e Americanas, por exemplo, empregam esses sistemas para sugerir produtos com base no comportamento dos usuários. Esses sistemas representam produtos e usuários

por meio de vetores numéricos, que codificam características como categorias, marcas e histórico de interação.

Para calcular a afinidade entre um usuário e um produto, uma das estratégias consiste em aplicar o produto de Hadamard entre seus vetores correspondentes. Essa operação multiplica, elemento a elemento, os dois vetores.

A seguir, apresentamos dois exemplos: um de baixa afinidade e outro de alta afinidade entre usuário e produto. Nos exemplos, o vetor $\mathbf{u}$ representa as preferências do usuário, enquanto $\mathbf{v}$ representa as características do produto. Suponha, por exemplo, que o nicho do produto seja filmes, e que as três coordenadas dos vetores representem, respectivamente: violência, romance e suspense. Se um filme apresenta alto teor de violência e o usuário aprecia essa característica, então a primeira coordenada de ambos os vetores será próxima de 1, e o Produto de Hadamard também terá valor próximo de 1 nessa posição. O mesmo acontece para as características romance e suspense. Ao final, calcula-se a soma dos elementos do vetor resultante, e a maior soma indica a combinação com maior afinidade entre o usuário e o produto.

Exemplo 6 (Baixa afinidade)**.** Considere o vetor de preferências de um usuário:

$$\mathbf{u}_1 = \begin{bmatrix} 0{,}9 \\ 0{,}2 \\ 0{,}8 \end{bmatrix} \quad \text{e o vetor de um produto:} \quad \mathbf{p}_1 = \begin{bmatrix} 0 \\ 1 \\ 0{,}1 \end{bmatrix}$$

Aplicando o produto de Hadamard, temos que

$$\mathbf{u}_1 \circ \mathbf{p}_1 = \begin{bmatrix} 0{,}9 \cdot 0 \\ 0{,}2 \cdot 1 \\ 0{,}8 \cdot 0{,}1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0{,}2 \\ 0{,}08 \end{bmatrix},$$

daí, a pontuação de afinidade resultante é baixa (soma $\approx 0{,}28$), indicando que esse produto tem pouca relação com os interesses do usuário.

Exemplo 7 (Alta afinidade)**.** Agora considere um segundo produto com vetor:

$$\mathbf{p}_2 = \begin{bmatrix} 1 \\ 0 \\ 0{,}5 \end{bmatrix}.$$

Aplicando o produto de Hadamard com o mesmo usuário, temos que:

$$\mathbf{u}_1 \circ \mathbf{p}_2 = \begin{bmatrix} 0{,}9 \cdot 1 \\ 0{,}2 \cdot 0 \\ 0{,}8 \cdot 0{,}5 \end{bmatrix} = \begin{bmatrix} 0{,}9 \\ 0 \\ 0{,}4 \end{bmatrix},$$

daí, a soma dos resultados dá $0{,}9+0+0{,}4 = 1{,}3$, indicando uma alta afinidade. Esse produto é mais alinhado com os interesses do usuário e, portanto, tem maior chance de ser recomendado.

Esse tipo de operação matemática simples é extremamente útil nos bastidores de sistemas inteligentes, contribuindo para uma experiência de compra mais personalizada e eficiente.

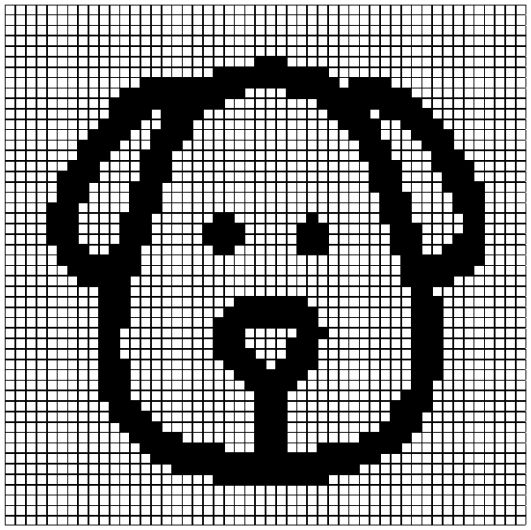


Figura 10 – Cachorrinho representado em uma matriz 50×50

Fonte: Imagem gerada com o auxílio da inteligência artificial ChatGPT, OpenAI, em [06/2025].

Outra aplicação do Produto de Hadamard está presente em sistemas de encriptação de imagens. Se associarmos valores numéricos a pixels organizados em uma matriz, podemos utilizar o produto de Hadamard para modificar esses pixels e, por meio de operações inversas, desfazer as modificações. Como exemplo ilustrativo, temos na figura 10 uma matriz 50×50 com pixels pretos e brancos (associados aos números 1 e 2), capaz de representar um cachorrinho. No capítulo seguinte, abordaremos com mais detalhes um método capaz de encriptar essa imagem.

O Produto de Hadamard também possui grande utilidade quando aplicado em sistemas comerciais. Tabelas com produtos, nas quais as matrizes representam lojas e os elementos correspondem aos preços dos produtos, podem ser utilizadas para identificar o estabelecimento mais vantajoso para a formação de parcerias comerciais. A vantagem do Produto de Hadamard em relação a outros métodos, nesses casos, é que visualizar a matriz como uma tabela permite, especialmente para máquinas, aplicar progressões específicas a cada elemento e gerar um resultado organizado, mantendo os novos valores nas mesmas posições da matriz original. Assim, por exemplo, ao se ter uma matriz com os preços e outra com as taxas de reajuste, o Produto de Hadamard entre elas já

fornece diretamente o valor final de cada produto, preservando sua posição na estrutura original. A seguir, serão apresentados múltiplos exemplos didáticos sobre o tema.

Exemplo 8. O Brasil, segundo Mann (2024), é um dos países com maior carga tributária sobre o consumo. Produtos diferentes recebem diferentes alíquotas de imposto, o que impacta diretamente o preço final pago pela população.

Vamos usar o Produto de Hadamard para calcular o preço final de alguns produtos populares no Brasil, considerando a carga de impostos aproximada sobre cada item.

Tabela com Preços Base e Impostos (aproximados)

Produto	**Preço Base (R$)**	**Carga Tributária**
Carro	70.000	43%
Moto	15.000	48%
Bicicleta	1.500	40%
Arroz	20	8%
Sabonete	5	37%

Matriz dos preços:

$$P = \begin{bmatrix} 70000 & 15000 & 1500 & 20 & 5 \end{bmatrix}.$$

Matriz dos fatores de imposto (1 + percentual):

$$I = \begin{bmatrix} 1{,}43 & 1{,}48 & 1{,}40 & 1{,}08 & 1{,}37 \end{bmatrix}.$$

Produto de Hadamard entre os preços e os fatores de imposto é:

$$\begin{aligned} P \circ I &= \begin{bmatrix} 70000 \cdot 1{,}43 & 15000 \cdot 1{,}48 & 1500 \cdot 1{,}40 & 20 \cdot 1{,}08 & 5 \cdot 1{,}37 \end{bmatrix} \\ &= \begin{bmatrix} 100.100 & 22.200 & 2.100 & 21{,}60 & 6{,}85 \end{bmatrix}. \end{aligned}$$

Assim, o valor final de cada produto após incidência dos impostos é:

- Carro: $R\$100.100$;
- Moto: $R\$22.200$;
- Bicicleta: $R\$2.100$;
- Arroz: $R\$21,60$;

- Sabonete: $R\$6,85$.

E o total de impostos pagos em cada item (valor final menos valor base).

$$\text{Impostos pagos: } \begin{bmatrix} 100.100 - 70.000 & 22.200 - 15.000 & 2.100 - 1.500 & 21{,}60 - 20 & 6{,}85 - 5 \end{bmatrix} = \begin{bmatrix} 30.100 & 7.200 & 600 & 1{,}60 & 1{,}85 \end{bmatrix}.$$

Exemplo 9. Fui à mercearia e anotei os preços dos produtos e as quantidades que desejo comprar em duas lojas diferentes. Agora, preciso calcular o valor total de cada item em cada loja e decidir onde vale mais a pena fazer as compras.

Tabela de Preços

Produto	**Loja A (R$)**	**Loja B (R$)**
Arroz	5,00	4,80
Feijão	6,50	6,30
Óleo	7,00	7,20
Leite	4,20	4,00
Sabão	2,00	2,20

Quantidades que desejo comprar:

Arroz	Feijão	Óleo	Leite	Sabão
2	1	3	4	5

Escrevemos os vetores (matrizes unidimensionais) com os preços da Loja A e Loja B, e o vetor de quantidades associados respectivamente a cada produto, mantendo a ordem de sua representação:

$$\text{Loja A: } P_A = \begin{bmatrix} 5{,}00 & 6{,}50 & 7{,}00 & 4{,}20 & 2{,}00 \end{bmatrix}$$
$$\text{Loja B: } P_B = \begin{bmatrix} 4{,}80 & 6{,}30 & 7{,}20 & 4{,}00 & 2{,}20 \end{bmatrix}$$
$$\text{Quantidade: } Q = \begin{bmatrix} 2 & 1 & 3 & 4 & 5 \end{bmatrix}$$

Realizamos o Produto de Hadamard entre os vetores de preço e quantidade para obter o custo total de cada item:

$$C_A = Q \circ P_A = \begin{bmatrix} 10{,}00 & 6{,}50 & 21{,}00 & 16{,}80 & 10{,}00 \end{bmatrix},$$

$$C_B = Q \circ P_B = \begin{bmatrix} 9{,}60 & 6{,}30 & 21{,}60 & 16{,}00 & 11{,}00 \end{bmatrix}.$$

A soma dos elementos determina a loja mais vantajosa.

Total em A: R$64,30,

Total em B: R$64,50.

Exemplo 10. Três amigos – Ana, Bruno e Carla – foram ao supermercado e compraram os mesmos produtos: arroz, feijão e macarrão. Quanto cada uma delas gastou?

Abaixo segue a representação em vetor (matriz unidimensional) e tabela do preço de cada produto, assim como da quantidade. A representação vetorial auxilia na aplicação do Produto de Hadamard.

Preço Unitário dos Produtos (em reais)

$$P = \begin{bmatrix} 5 & 7 & 4 \end{bmatrix}$$

	Arroz	Feijão	Macarrão
Preço	R$ 5	R$ 7	R$ 4

Quantidade comprada por cada pessoa

$$Q = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 2 & 1 \\ 3 & 0 & 2 \end{bmatrix}$$

	Arroz	Feijão	Macarrão
Ana	2	1	3
Bruno	1	2	1
Carla	3	0	2

Considere que a matriz de preços P foi replicada em 3 linhas, já que os valores eram os mesmos para as compras dos 3. Calcule a matriz resultante da operação $P \circ Q$.

$$P \circ Q = \begin{bmatrix} 2 \cdot 5 & 1 \cdot 7 & 3 \cdot 4 \\ 1 \cdot 5 & 2 \cdot 7 & 1 \cdot 4 \\ 3 \cdot 5 & 0 \cdot 7 & 2 \cdot 4 \end{bmatrix} = \begin{bmatrix} 10 & 7 & 12 \\ 5 & 14 & 4 \\ 15 & 0 & 8 \end{bmatrix}$$

A soma das linhas são os gastos de cada pessoa. Totais:

- Ana: $10 + 7 + 12 =$ **R$ 29**;
- Bruno: $5 + 14 + 4 =$ **R$ 23**;
- Carla: $15 + 0 + 8 =$ **R$ 23**.

Portanto, estudadas as propriedades indispensáveis do Produto de Hadamard e apresentada algumas de suas aplicações, apresentaremos, na seção seguinte, uma interessante relação entre o Produto de Hadamard e o produto usual de matrizes. Entretanto, faz-se necessário, antes disso, definir alguns conceitos matemáticos que serão utilizados. Entre eles, destacamos a permutação de matrizes, a qual será definida conforme apresentado por Horn e Johnson (2012).

3.3 Matrizes de permutação

Definição 3.3. *Uma matriz quadrada P é uma matriz de permutação se exatamente uma entrada em cada linha e coluna for igual a 1 e todas as outras entradas forem 0. A multiplicação por tais matrizes realiza uma permutação das linhas ou colunas da matriz multiplicada.*

Por exemplo, podemos considerar

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix},$$

que ilustra como uma *matriz de permutação* produz uma permutação das linhas (entradas) de um vetor: ela envia a primeira entrada para a segunda posição, a segunda entrada para a primeira posição e deixa a terceira entrada na terceira posição.

A multiplicação à esquerda de uma matriz $A \in \mathbb{M}_{m,n}$ por uma *matriz de permutação* $P \in \mathbb{M}_{m,m}$ permuta as linhas de A, enquanto a multiplicação à direita de A por uma matriz de permutação $P \in \mathbb{M}_{n,n}$ permuta as colunas de A.

O determinante de uma *matriz de permutação* é ± 1, logo, matrizes de permutação são não singulares. Embora matrizes de permutação não precisem comutar, o produto de duas matrizes de permutação é novamente uma *matriz de permutação*.

3.4 Conexão entre os produtos de Hadamard e produtos matriciais

Esta seção foi baseada no trabalho de Caro-Lopera, Leiva e Balakrishnan (2012), no qual apontamos uma conexão direta entre o Produto de Hadamard e o produto usual

de matrizes. Antes de enunciarmos o teorema principal deste capítulo, apresentaremos a definição formal do produto usual de matrizes e, para nosso teorema, definiremos a construção de dois tipos especiais de matrizes, essenciais para a formulação dos dois produtos.

Definição 3.4. ***(Produto Usual de Matrizes):*** *Sejam $A = [a_{ij}] \in M_{m\times n}(\mathbb{R})$ e $B = [b_{jk}] \in M_{n\times p}(\mathbb{R})$. O produto usual de matrizes, denotado por $A \cdot B$, é a matriz $C = [c_{ik}] \in M_{m\times p}(\mathbb{R})$ tal que:*

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}, \quad \textit{para todo } 1 \leq i \leq m,\ 1 \leq k \leq p,$$

ou seja, a entrada c_{ik} da matriz resultante é obtida multiplicando a i-ésima linha de A pela k-ésima coluna de B e somando os produtos correspondentes.

Definição 3.5. *Dada a matriz $A = [a_{ij}] \in M_{k\times k}(\mathbb{R})$, considere o conjunto $P_{1\ 2\cdots k}$ de permutações cíclicas de $1\ 2\cdots k$ dado por:*

$$P_{1\ 2\cdots k} = \{(1\ 2\ \ldots\ k), (2\ 3\ \ldots\ k\ 1), \ldots, (k\ 1\ 2\ \ldots\ (k{-}1))\}. \tag{3.6}$$

Se a_i é a i-ésima coluna da matriz A, então para um elemento particular $p = p_1\ p_2\ \ldots\ p_k \in P_{1\ 2\cdots k}$ na equação anterior, definimos:

$$A_{(p)} = (a_{p_1} \mid a_{p_2} \mid \cdots \mid a_{p_k}), \tag{7}$$

ou seja, $A_{(p)}$ é a matriz A com as colunas permutadas de acordo com a permutação $p = p_1\ p_2\ \ldots\ p_k$.

Exemplo 11. Para a permutação $3\ 4 \ldots k\ 1\ 2$, temos:

$$A_{(3\ 4\ \ldots\ k\ \ 2)} = \begin{pmatrix} a_{13} & a_{14} & \cdots & a_{1k} & a_{11} & a_{12} \\ a_{23} & a_{24} & \cdots & a_{2k} & a_{21} & a_{22} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{(k-1)3} & a_{(k-1)4} & \cdots & a_{(k-1)k} & a_{(k-1)1} & a_{(k-1)2} \\ a_{k3} & a_{k4} & \cdots & a_{kk} & a_{k1} & a_{k2} \end{pmatrix}.$$

Se considerarmos A como a matriz identidade, então $A_{(p)}$ será uma matriz de permutação, introduzida na seção 3.3.

Definição 3.6. *Dada a matriz $B = [b_{ij}] \in M_{k\times k}(\mathbb{R})$, definimos:*

$$B_{[p]} = \begin{pmatrix} b_{p_1 1} & b_{p_2 2} & \cdots & b_{p_k k} \\ b_{p_1 1} & b_{p_2 2} & \cdots & b_{p_k k} \\ \vdots & \vdots & \ddots & \vdots \\ b_{p_1 1} & b_{p_2 2} & \cdots & b_{p_k k} \end{pmatrix}. \tag{8}$$

Ou seja, cada coluna j contém repetidamente o valor $b_{p_i j}$, formando uma matriz onde cada coluna é formada pelo mesmo elemento. O objetivo da existencia de $B_{[p]}$ é ser uma matriz com linhas iguais, porém indexadas a permutação p.

Com essa notação, temos o seguinte teorema:

Teorema 3.7. *Sejam $A = [a_{ij}]$, $B = [b_{ij}] \in M_{k\times k}(\mathbb{R})$. Então,*

$$A \cdot B = \sum_p A_{(p)} \circ B_{[p]} = \sum_p (A \cdot I_{(p)}) \circ B_{[p]}, \tag{3.7}$$

onde $A_{(p)}$ e $B_{[p]}$ são definidos nas equações 7 e 8, respectivamente, para cada permutação $p \in P_{1\ 2\cdots k}$.

Demonstração. Desde que, $A = [a_{ij}]$ e $B = [b_{ij}]$ são matrizes em $M_{k\times k}(\mathbb{R})$, temos, pela Definição 3.4,

$$A{\cdot}B = \begin{pmatrix} \sum\limits_{j=1}^{k} a_{1j}b_{j1} & \sum\limits_{j=1}^{k} a_{1j}b_{j2} & \cdots & \sum\limits_{j=1}^{k} a_{1j}b_{jk} \\ \sum\limits_{j=1}^{k} a_{2j}b_{j1} & \sum\limits_{j=1}^{k} a_{2j}b_{j2} & \cdots & \sum\limits_{j=1}^{k} a_{2j}b_{jk} \\ \vdots & \vdots & \ddots & \vdots \\ \sum\limits_{j=1}^{k} a_{kj}b_{j1} & \sum\limits_{j=1}^{k} a_{kj}b_{j2} & \cdots & \sum\limits_{j=1}^{k} a_{kj}b_{jk} \end{pmatrix} \overset{1}{=} \left(\sum_{j=1}^{k} a_{ij}b_{j1} \;\middle|\; \sum_{j=1}^{k} a_{ij}b_{j2} \;\middle|\; \cdots \;\middle|\; \sum_{j=1}^{k} a_{ij}b_{jk} \right).$$

A igualdade **(1)** representa o produto usual de matrizes escrito com foco na estrutura por colunas, conforme a notação utilizada na equação 7. Esta forma de representar o produto matricial destaca os elementos iniciais de cada coluna — os quais serão objeto das permutações — enquanto abstrai os elementos das demais linhas, que serão rearranjados conjuntamente com suas respetivas colunas.

O objetivo desta mudança de notação é facilitar a visualização e manipulação das permutações cíclicas, tornando o processo mais claro e intuitivo no contexto da decomposição apresentada no Teorema 3.7.

O produto usual de matrizes $A \cdot B$ se decompõe unicamente como a soma de k matrizes que chamaremos de C_p, onde, $p = p_1\ p_2 \cdots p_k \in P_{1\ 2\cdots k}$. A fim de facilitar a visualização da construção da matriz C_p para o leitor, fazemos o produto usua de matrizes entre duas matrizes genéricas. Logo, sejam as matrizes:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \quad B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}$$

O produto usual $A \cdot B = C$ é dado por:

$$C = A{\cdot}B = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} & a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33} \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} & a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} & a_{31}b_{13} + a_{32}b_{23} + a_{33}b_{33} \end{bmatrix}$$

Na matriz acima, destacam-se em vermelho o primeiro somando da primeira coluna, o segundo somando da segunda coluna e o terceiro somando da terceira coluna, caso base da construção de C_p.

A matriz C_p será construída de forma decomposta da seguinte maneira: primeira matriz $C_{1\ 2\ \ldots\ k}$ é obtida pegando-se o primeiro somando[1] da primeira coluna, o segundo somando da segunda coluna, e assim por diante. Isto é:

$$C_{1\ 2\ldots k} = (a_{11}b_{11} \mid a_{12}b_{22} \mid \cdots \mid a_{1k}b_{kk}) = A_{(1\ 2\ldots k)} \circ B_{[1\ 2\ldots k]}.$$

Em outras palavras, $C_{1\ 2\ldots k}$ é construída extraindo os somandos de cada coluna de acordo com a permutação $1\ 2 \cdots k$. A segunda matriz é selecionada de acordo com a permutação $2\ 3\ \cdots\ k\ 1$; isto é, selecionando o segundo somando da primeira coluna, o terceiro somando da segunda coluna, e assim por diante até o primeiro somando da última coluna. Assim, expandindo as matrizes $C_{(2\ 3\ldots k\ 1)}, A_{(2\ 3\ldots k\ 1)}, B_{[2\ 3\ldots k\ 1]}$, temos:

$$C_{(2\ 3\ldots k\ 1)} = \begin{pmatrix} a_{12}b_{21} & a_{13}b_{32} & \cdots & a_{1k}b_{k(k-1)} & a_{11}b_{1k} \\ a_{22}b_{21} & a_{23}b_{32} & \cdots & a_{2k}b_{k(k-1)} & a_{21}b_{1k} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k2}b_{21} & a_{k3}b_{32} & \cdots & a_{kk}b_{k(k-1)} & a_{k1}b_{1k} \end{pmatrix},$$

$$A_{(2\ 3\ldots k\ 1)} = \begin{pmatrix} a_{12} & a_{13} & \cdots & a_{1k} & a_{11} \\ a_{22} & a_{23} & \cdots & a_{2k} & a_{21} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{k2} & a_{k3} & \cdots & a_{kk} & a_{k1} \end{pmatrix},$$

$$B_{[2\ 3\ldots k\ 1]} = \begin{pmatrix} b_{21} & b_{32} & \cdots & b_{k(k-1)} & b_{1k} \\ b_{21} & b_{32} & \cdots & b_{k(k-1)} & b_{1k} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{21} & b_{32} & \cdots & b_{k(k-1)} & b_{1k} \end{pmatrix}.$$

Portanto, diante das expansões acima, é imediato concluir que:

$$C_{(2\ 3\ldots k\ 1)} = \left(a_2b_{21} \,\middle|\, a_3b_{32} \,\middle|\, \cdots \,\middle|\, a_kb_{k(k-1)} \,\middle|\, a_1b_{1k}\right) = A_{(2\ 3\ldots k\ 1)} \circ B_{[2\ 3\ldots k\ 1]}. \tag{3.8}$$

[1] Somando é cada elemento de uma soma. Por exemplo, em $1 + 2 + 3 + 4$ o conjunto dos somandos é $S = 1, 2, 3, 4$

Seguindo esse procedimento e considerando o conjunto completo de k permutações cíclicas de $1\ 2\cdots k$ na equação 3.6, obtemos a matriz $(k-1)$-ésima como

$$C_{(k-1)\ k\ 1\cdots(k-3)\ (k-2)} = A_{((k-1)\ k\ 1\cdots(k-3)\ (k-2))} \circ B_{[((k-1)\ k\ 1\cdots(k-3)\ (k-2))]}. \tag{3.9}$$

Finalmente, a matriz correspondente à permutação final $k\ 1\cdots(k-2)\ (k-1)$ é formada pelos somandos restantes como:

$$\begin{aligned} C_{k\ 1\ldots(k-2)\ (k-1)} &= (a_k b_{k1} \mid a_1 b_{12} \mid \cdots \mid a_{(k-2)} b_{(k-2)(k-1)} \mid a_{(k-1)} b_{(k-1)k}) \\ &= A_{(k\ 1\ldots(k-2)\ (k-1))} \circ B_{[k\ 1\ \ldots(k-2)\ (k-1)]}. \end{aligned} \tag{3.10}$$

Assim, temos:

$$\begin{aligned} A \cdot B = {} & A_{(1\ 2\ldots k)} \circ B_{[1\ 2\ldots k]} + A_{(2\ 3\ldots k\ 1)} \circ B_{[2\ 3\ldots k\ 1]} + A_{(3\ 4\ldots k\ 1\ 2)} \circ B_{[3\ 4\ldots k\ 1\ 2]} + \cdots \\ & + A_{((k-1)\ k\ 1\ldots(k-3)\ (k-2))} \circ B_{[((k-1)\ k\ 1\ldots(k-3)\ (k-2))]} \\ & + A_{(k\ 1\ldots(k-2)\ (k-1))} \circ B_{[k\ 1\ldots(k-2)\ (k-1)]} \end{aligned} \tag{3.11}$$

que é o resultado requerido.

■

Exemplo 12. Vamos verificar o Teorema 3.7 no caso em que $k = 2$. Sejam:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}.$$

O produto usual das matrizes é:

$$A \cdot B = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

As permutações cíclicas de ordem 2 são $p = (1, 2)$ e $p = (2, 1)$. Vamos calcular separadamente os produtos de Hadamard $A_{(p)} \circ B_{[p]}$ para cada permutação:

Para $p = (1, 2)$:

$$A_{(1\ 2)} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B_{[1\ 2]} = \begin{pmatrix} b_{11} & b_{22} \\ b_{11} & b_{22} \end{pmatrix},$$

$$A_{(1\ 2)} \circ B_{[1\ 2]} = \begin{pmatrix} a_{11}b_{11} & a_{12}b_{22} \\ a_{21}b_{11} & a_{22}b_{22} \end{pmatrix}.$$

Para $p = (2\ 1)$:

$$A_{(2\ 1)} = \begin{pmatrix} a_{12} & a_{11} \\ a_{22} & a_{21} \end{pmatrix}, \quad B_{[2\ 1]} = \begin{pmatrix} b_{21} & b_{12} \\ b_{21} & b_{12} \end{pmatrix},$$

$$A_{(2\ 1)} \circ B_{[2\ 1]} = \begin{pmatrix} a_{12}b_{21} & a_{11}b_{12} \\ a_{22}b_{21} & a_{21}b_{12} \end{pmatrix}.$$

Somando os dois resultados:

$$A \cdot B = A_{(1\ 2)} \circ B_{[1\ 2]} + A_{(2\ 1)} \circ B_{[2\ 1]} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{12}b_{22} + a_{11}b_{12} \\ a_{21}b_{11} + a_{22}b_{21} & a_{22}b_{22} + a_{21}b_{12} \end{pmatrix},$$

que coincide exatamente com o produto usual.

Exemplo 13. Vamos verificar o Teorema 3.7 para o caso em que $k = 3$.

Sejam:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \text{ e } \quad B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix},$$

O produto usual das matrizes é:

$$A \cdot B = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} & a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33} \\ a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31} & a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32} & a_{31}b_{13} + a_{32}b_{23} + a_{33}b_{33} \end{pmatrix}.$$

As permutações cíclicas de ordem 3 são (1 2 3), (2 3 1) e (3 1 2). Vamos calcular os produtos de Hadamard para cada permutação.

Para $p = (1\ 2\ 3)$:

$$A_{(1\ 2\ 3)} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \quad B_{[1\ 2\ 3]} = \begin{pmatrix} b_{11} & b_{22} & b_{33} \\ b_{11} & b_{22} & b_{33} \\ b_{11} & b_{22} & b_{33} \end{pmatrix},$$

$$A_{(1\ 2\ 3)} \circ B_{[1\ 2\ 3]} = \begin{pmatrix} a_{11}b_{11} & a_{12}b_{22} & a_{13}b_{33} \\ a_{21}b_{11} & a_{22}b_{22} & a_{23}b_{33} \\ a_{31}b_{11} & a_{32}b_{22} & a_{33}b_{33} \end{pmatrix}.$$

Para $p = (2\ 3\ 1)$:

$$A_{(2\ 3\ 1)} = \begin{pmatrix} a_{12} & a_{13} & a_{11} \\ a_{22} & a_{23} & a_{21} \\ a_{32} & a_{33} & a_{31} \end{pmatrix}, \quad B_{[2\ 3\ 1]} = \begin{pmatrix} b_{21} & b_{32} & b_{13} \\ b_{21} & b_{32} & b_{13} \\ b_{21} & b_{32} & b_{13} \end{pmatrix},$$

$$A_{(2\ 3\ 1)} \circ B_{[2\ 3\ 1]} = \begin{pmatrix} a_{12}b_{21} & a_{13}b_{32} & a_{11}b_{13} \\ a_{22}b_{21} & a_{23}b_{32} & a_{21}b_{13} \\ a_{32}b_{21} & a_{33}b_{32} & a_{31}b_{13} \end{pmatrix}.$$

Para $p = (3\ 1\ 2)$:

$$A_{(3\ 1\ 2)} = \begin{pmatrix} a_{13} & a_{11} & a_{12} \\ a_{23} & a_{21} & a_{22} \\ a_{33} & a_{31} & a_{32} \end{pmatrix}, \quad B_{[3\ 1\ 2]} = \begin{pmatrix} b_{31} & b_{12} & b_{23} \\ b_{31} & b_{12} & b_{23} \\ b_{31} & b_{12} & b_{23} \end{pmatrix},$$

$$A_{(3\ 1\ 2)} \circ B_{[3\ 1\ 2]} = \begin{pmatrix} a_{13}b_{31} & a_{11}b_{12} & a_{12}b_{23} \\ a_{23}b_{31} & a_{21}b_{12} & a_{22}b_{23} \\ a_{33}b_{31} & a_{31}b_{12} & a_{32}b_{23} \end{pmatrix}.$$

Somando as três contribuições:

$$A \cdot B = A_{(1\ 2\ 3)} \circ B_{[1\ 2\ 3]} + A_{(2\ 3\ 1)} \circ B_{[2\ 3\ 1]} + A_{(3\ 1\ 2)} \circ B_{[3\ 1\ 2]}$$

que coincide exatamente com o produto usual.

Uma expansão similar de $A \cdot B$, quando as matrizes A e B não são quadradas, também é de interesse. O teorema e sua demonstração podem ser consultados no trabalho de Caro-Lopera, Leiva e Balakrishnan (2012) de onde se originou essa seção, mas não serão abordados aqui por fugirem do escopo do trabalho.

Teorema 3.8. *Sejam $A = [a_{ij}] \in M_{n\times k}(\mathbb{R})$ e $B = [b_{ij}] \in M_{k\times n}(\mathbb{R})$, com $n \leq k$. Então,*

$$A \cdot B = \sum_p A_{(p)} \circ B_{[p]} = \sum_p (A \cdot I_{(p)}) \circ B_{[p]},$$

onde a soma percorre todas as permutações cíclicas $p = p_1\ p_2\ \cdots\ p_n$ (consistindo nos primeiros n índices) de $P_{1\ 2\ \ldots\ n\ \ldots\ k}$. Para uma permutação particular $p = p_1\ p_2\ \cdots, p_n \in P_{1\ 2\ \ldots\ n\ \ldots\ k}$, $A_{(p)}$ é como dado na construção 7, com k substituído por n, e $B_{[p]}$ é como na construção 8.

Como um exemplo simples, tomemos:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{bmatrix}.$$

Aqui, $P_{1\ 2\ 3} = \{123\ 231\ 312\}$ como de costume, mas as permutações que consideramos têm apenas as duas primeiras partes, ou seja, $p = 12\ 23$ ou 31. Então:

$$A \cdot B = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31} & a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32} \\ a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31} & a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \circ \begin{bmatrix} b_{11} & b_{12} \\ b_{11} & b_{22} \end{bmatrix} + \begin{bmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{bmatrix} \circ \begin{bmatrix} b_{21} & b_{22} \\ b_{21} & b_{32} \end{bmatrix} + \begin{bmatrix} a_{13} & a_{11} \\ a_{23} & a_{21} \end{bmatrix} \circ \begin{bmatrix} b_{31} & b_{12} \\ b_{31} & b_{12} \end{bmatrix}$$

$$= A_{(12)} \circ B_{[12]} + A_{(23)} \circ B_{[23]} + A_{(31)} \circ B_{[31]}$$

$$= (A \cdot I_{(12)}) \circ B_{[12]} + (A \cdot I_{(23)}) \circ B_{[23]} + (A \cdot I_{(31)}) \circ B_{[31]},$$

onde

$$I_{(12)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad I_{(23)} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I_{(31)} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix},$$

correspondentes às duas primeiras colunas de $I_{(123)}$, $I_{(231)}$ e $I_{(312)}$, respectivamente.

4 Criptografia

Ao longo da história, a humanidade desenvolveu diversas estratégias para proteger a informação. Inicialmente, essas estratégias visavam garantir a privacidade em comunicações pessoais, políticas ou militares. Com o avanço das tecnologias de comunicação e a popularização da internet, a necessidade de proteger dados tornou-se ainda mais urgente, expandindo-se para o cotidiano de bilhões de pessoas ao redor do mundo. Hoje, práticas como a criptografia deixaram de ser exclusividade de especialistas ou governos e tornaram-se essenciais para qualquer usuário comum de dispositivos digitais.

Neste capítulo, discutimos algumas das principais técnicas de ocultação de mensagens, com foco especial nas estratégias criptográficas. A primeira parte do capítulo apresenta os conceitos fundamentais de esteganografia e criptografia, explorando desde os métodos utilizados na antiguidade até os sistemas de transposição clássicos, como a cifra cerca de ferrovia e o citale espartano. Por meio de exemplos didáticos, mostramos como essas técnicas embaralham a informação com base em padrões previamente combinados, garantindo que apenas o destinatário legítimo seja capaz de interpretá-la corretamente. As informações históricas contidas nessa primeira fase do capítulo foram retiradas por completo do livro Singh (2001).

Na segunda parte do capítulo, avançamos para uma abordagem mais moderna e matemática da criptografia, utilizando o Produto de Hadamard como ferramenta para encriptação. A proposta é aplicar esse produto matricial em um processo de codificação de imagens, aproveitando suas propriedades para embaralhar os dados visuais de maneira eficiente. Este exercício não apenas introduz uma aplicação concreta do conteúdo matemático, como também demonstra o potencial interdisciplinar da criptografia, articulando saberes da Matemática, da computação e da segurança da informação.

Ao final deste capítulo, o leitor terá uma visão abrangente da evolução dos métodos de ocultação da escrita, bem como uma introdução prática ao uso de operações matriciais em aplicações criptográficas. Essa abordagem busca contribuir para o desenvolvimento de uma compreensão crítica sobre o papel da Matemática na proteção de dados em nossa sociedade digital.

4.1 Relatos modernos

Atualmente, a criptografia está presente no dia a dia do cidadão comum como nunca antes na história da humanidade. Ao ouvirem o termo, muitas pessoas associam-no imediatamente à segurança digital — reflexo da ampla utilização da criptografia nos

sistemas de comunicação modernos. Ao enviar uma mensagem no WhatsApp, por exemplo, somos informados pela própria plataforma de que as conversas "são protegidas com a criptografia de ponta a ponta". De forma clara e acessível, a empresa explica:

> A criptografia de ponta a ponta do WhatsApp protege as suas conversas com outras pessoas no WhatsApp Messenger, garantindo que as mensagens e ligações fiquem somente entre você e a pessoa com quem conversar. Ninguém mais pode ler, ouvir ou compartilhar suas conversas, nem mesmo o WhatsApp. Com a criptografia de ponta a ponta, as mensagens e ligações são protegidas com um cadeado exclusivo e somente você e a pessoa que recebe a mensagem têm acesso à chave especial para destrancá-lo e ler as mensagens. (WhatsApp, 2025)

Na época em que esse sistema foi incorporado à aplicação, era comum ver decisões judiciais, em várias partes do mundo, exigindo que a empresa fornecesse o conteúdo das conversas dos seus utilizadores. No Brasil, por exemplo, em 2015, o juiz Luís Moura Correia, da Central de Inquéritos da Comarca de Teresina, determinou que as operadoras de telefonia suspendessem temporariamente, em todo o território nacional, o acesso ao WhatsApp (G1 Piauí, 2015). Segundo o Núcleo de Inteligência, essa medida judicial foi emitida em 11 de fevereiro, após a empresa se recusar a fornecer informações para uma investigação policial.

Um caso ainda mais emblemático envolveu a Apple e o seu dispositivo iPhone. De acordo com G1 Tecnologia (2016), após a empresa ter recusado colaborar voluntariamente, a Justiça Federal dos Estados Unidos ordenou que a Apple burlasse o seu próprio sistema de criptografia implementado no iPhone. A Apple argumentou que revelar os segredos do sistema colocaria em risco a segurança de todos os seus dispositivos e utilizadores a nível mundial, comprometendo assim a confiança e o valor da marca.

Por fim, tratando de valor de mercado, vale a pena mencionar o caso dos Bitcoins perdidos. Segundo InfoMoney (2024), existe o equivalente a cinco Petrobras em Bitcoins perdidos — grande parte dos quais jamais será recuperada. Este fenômeno ocorre quando o proprietário da criptomoeda, que optou por manter a custódia das suas próprias chaves criptográficas, as perde ou esquece. Sem essa chave, o acesso às moedas torna-se impossível, sobretudo por se tratar de um sistema descentralizado, sem qualquer órgão ou governo que o controle. Se, por absurdo, alguém conseguir quebrar esse sistema criptográfico e aceder a esses Bitcoins perdidos, o valor de todas as moedas existentes entraria em colapso.

Estes casos demonstram que o valor da criptografia está diretamente ligado ao segredo por trás do processo de codificação dos dados. Uma vez comprometida a chave, todas as informações protegidas por aquele sistema ficam vulneráveis, e o valor da criptografia — a sua capacidade de garantir a segurança dos dados — perde-se.

Ao longo da história, diferentes métodos de proteção da informação foram sendo desenvolvidos, desde técnicas rudimentares até algoritmos modernos. A evolução dessas práticas acompanha a necessidade humana de guardar segredos — seja para fins pessoais, políticos, militares ou económicos.

Neste contexto, torna-se essencial compreender as diversas estratégias utilizadas ao longo dos séculos para ocultar mensagens. Entre essas estratégias, destacam-se a esteganografia e a criptografia, duas formas distintas — e muitas vezes complementares — de proteção da informação. A seguir, exploraremos os principais tipos de ocultação de escrita, desde os métodos clássicos usados na Antiguidade até os sistemas mais sofisticados que lançaram as bases para a criptografia moderna.

4.2 Tipos de ocultação de escrita

Segundo Singh (2001), a arte de comunicar-se secretamente através de ocultação da mensagem é conhecida como esteganografia, nome derivado das palavras gregas steganos, que significa coberto, e graphein, que significa escrever. Os antigos chineses, por exemplo, escreviam mensagens em seda fina e faziam dela uma pequena bolinha de papel coberta com cera. O mensageiro engolia a bolinha de cera para transportar a mensagem de forma segura. No século XVI o cientista italiano Giovanni Porta descreveu como esconder uma mensagem dentro de um ovo cozido. Fabricava-se uma tinta com uma onça de alume e um quartilho de vinagre e então escrevendo na casca do ovo. Essa tinta especial penetrava a casca do ovo e se fixava na clara endurecida. O ovo poderia ser transportado sem que a mensagem fosse vista e para lê-la bastava descascar o ovo. No primeiro século depois de Cristo, Plínio, o velho, ja explicava como a seiva da planta titímalo era transparente quando aplicada sobre uma superfície mas marrom após aquecida, de modo que poderia ser uma ferramenta esteganográfica. Após o século XX, sem acesso a esse tipo de tinta, espiões usavam a própria urina que conseguia cumprir com essa função.

Paralelo ao desenvolvimento da esteganografia está o surgimento da criptografia, derivada da palavra grega kriptos, que significa “oculto”. Diferente da esteganografia a criptografia não tem preocupação nenhuma em esconder a existência de uma mensagem, ela tem por objetivo esconder o significado para terceiros, usando um processo conhecido como encriptação. Este processo consiste na elaboração de um protocolo de embaralhamento da informação a ser conhecida pelo emissor e receptor da mensagem. Com isso, ao recebê-la o receptor poderá reverter o processo de embaralhamento e ter acesso a seu significado. Essa é a vantagem da criptografia em relação a esteganografia, pois caso a mensagem pare nas mãos de terceiros, não conseguirão lê-la ou terão de perder muito tempo para quebrar a encriptação, dando vantagem para o emissor.

Algumas vezes a criptografia e a esteganografia eram aplicadas juntas a fim de dar dupla camada de proteção a mensagem. Um bom exemplo disso é o microponto, usado da Segunda Guerra Mundial por agentes alemães. A prática consistia em reduzir fotograficamente uma página de texto até transformá-la em um ponto. Segundo Superinteressante (2020), o ponto poderia ter menos de 1 milímetro. O primeiro microponto foi descoberto pelo FBI em 1941, atentos ao brilho do filme nos pontos encontrado nas cartas. Uma resposta dos alemães ao avanço na investigação dos americanos foi codificar a mensagem antes de transformá-las em microponto, adicionando duplava camada de proteção a mensagem.

4.2.1 Criptografia por transposição

A criptografia, por usa vez, pode ser dividida em dois ramos: transposição e substituição. Na transposição há uma troca na posição das letras, gerando um anagrama. É um sistema que só proporciona segurança quando se trata de mensagens grandes. Segundo MORGADO et al. (1991), dado um conjunto com n objetos distintos, o número total de maneiras possíveis de ordená-los (isto é, o número de permutações desses n elementos) é dado por:

$$P(n) = n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1, \tag{4.1}$$

onde o símbolo $n!$, chamado de *fatorial de* n, representa o produto de todos os inteiros positivos de 1 até n.

Vejamos dois exemplos que ilustram bem o quão grande precisa ser uma mensagem para que esse sistema criptográfico seja seguro. Suponhamos que iremos criptografar a palavra "boi". Ela é composta por 3 letras, logo existem $3! = 6$ permutações possíveis, são elas: boi, bio, ibo, obi, oib, iob.

A função fatorial cresce de forma extremamente rápida com o aumento de n. Esse fenômeno é conhecido como explosão combinatória. Mesmo para valores relativamente pequenos de n, o valor de $n!$ se torna muito grande.

Por exemplo:

$$\begin{aligned} 5! &= 120 \\ 10! &= 3\,628\,800 \\ 15! &= 1\,307\,674\,368\,000 \\ 20! &= 2\,432\,902\,008\,176\,640\,000. \end{aligned}$$

Esse crescimento é muito mais rápido do que funções polinomiais (como n^2, n^3) e até mesmo exponenciais moderadas (como 2^n). Essa característica torna o cálculo de

permutações e combinações com grandes n computacionalmente custoso. Por exemplo, considere a frase **O boi comeu todo o capim que estava no campo**, ela contém 35 letras e existem mais de 50.000.000.000.000.000.000.000.000.000.000 arranjos distintos. Se uma pessoa pudesse verificar uma disposição por segundo, e se todas as pessoas no mundo trabalhassem dia e noite, ainda assim levaria mais de mil vezes o tempo de existência do universo para checar todos os arranjos possíveis.[1] Logo, podemos concluir que para frases com uma quantidade relativamente grande de letras a criptografia por transposição é segura, entretanto, é necessário ter atenção ao padrão de embaralhamento escolhido e no compartilhamento desse padrão apenas com o destinatário, pois sem ele a descriptação torna-se impossível.

Um didático exemplo desse sistema de encriptação é a cifra cerca de ferrovia, uma cifra de transposição em que a mensagem é escrita em forma de zigue-zague sobre várias linhas (ou trilhos), e em seguida é lida linha por linha para formar a mensagem cifrada.

Exemplo 14. Mensagem original:

```
ATAQUE AO AMANHECER
```

Removendo os espaços:

```
ATAQUEAOAMANHECER
```

Distribuímos os caracteres alternadamente entre 2 linhas:

1ª linha:	A	A	U	A	A	A	H	C	R
2ª linha:	T	Q	E	O	M	N	E	E	

Mensagem cifrada:

```
AAUAAAHCRTQEOMNEE
```

Para reverter a cifra, divide-se a mensagem em dois grupos (um para cada trilho), e reconstrói-se a sequência alternando as letras de cada trilho. Essa cifra é simples de aplicar e reverter, e é frequentemente usada para fins educativos e lúdicos, embora não ofereça segurança real contra análise criptográfica. O padrão de embaralhamento pode sofrer alterações e a dificuldade e segurança pode ser aumentada adicionando trilhos.

Outra forma de transposição envolve o primeiro aparelho criptográfico militar, o *citale* espartano, que consiste em um dos mais antigos dispositivos de criptografia conhecidos, utilizado por volta do século V a.C. pelos espartanos para enviar mensagens

[1] Estima-se que o universo tenha aproximadamente 435.400.000.000.000.000 segundos de existência — quase meio quintilhão de segundos!

secretas em tempos de guerra. Trata-se de um cilindro onde uma fita era enrolada em espiral. A mensagem era escrita ao longo do cilindro, linha por linha, e depois desenrolada. A mensagem parecia embaralhada até que fosse enrolada em outro cilindro de mesmo diâmetro. Portanto, para este método, o cilindro com seu diâmetro especificado era a chave de embaralhamento. Emissor e remetente deveriam possuir um com mesmas características métricas.

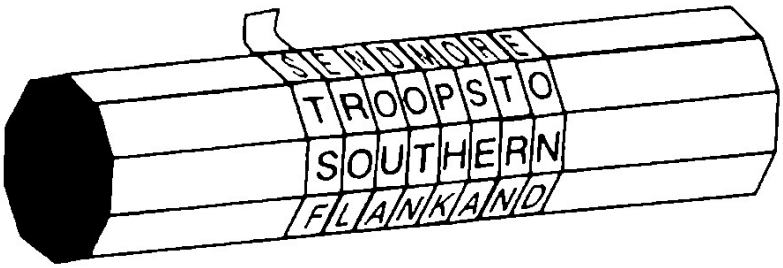


Figura 11 – Representação gráfica de um Citale Espartano

Fonte: (SINGH, 2001)

Exemplo 15. Vamos usar a seguinte mensagem (sem espaços):

`ATAQUEAOAMANHECER`

Suponha que o comprimento da fita permita 5 colunas. Vamos organizar a mensagem em uma matriz com 5 colunas (como se ela tivesse sido escrita enrolando-se a fita em torno do citale):

A	T	A	Q	U
E	A	O	A	M
A	N	H	E	C
E	R			

(Letras em branco representam espaços não utilizados, já que a mensagem não preenche uma matriz 100%)

Mensagem original:

`ATAQUEAOAMANHECER`

Mensagem cifrada (fita desenrolada):

A	E	A	E	T	A	N	R	A	O	H		Q	A	E		U	M	C	

Mensagem cifrada final: `AEAERTAONRAOHQAEUMC`

Sem saber o número de colunas (ou o diâmetro do bastão), é muito difícil decifrar a mensagem. Isso faz do citale um exemplo histórico importante de cifra por transposição, onde a segurança está na reorganização da mensagem, e não na substituição de caracteres.

4.2.2 Criptografia por substituição

O citale espartano foi o primeiro método de criptografia por transposição que se tem registro, e, segundo Singh (2001), uma das primeiras descrições de código por substituição:

> [...] aparece no *Kama-sutra*, um texto escrito no século IV pelo estudioso brâmane Vatsyayana, baseado em manuscritos que datam do século IV a.C. O *Kama-sutra* recomenda que as mulheres devem estudar 64 artes, incluindo culinária, vestuário, massagem e preparação de perfumes. A lista também inclui algumas artes menos óbvias, incluindo magia, xadrez, encadernação de livros e carpintaria. O número 45 da lista é a *mlecchita-vikalpa*, a arte da escrita secreta, justificada de modo a ajudar as mulheres a esconderem os detalhes de seus relacionamentos. Uma das técnicas recomendadas envolve o emparelhamento ao acaso das letras do alfabeto, substituindo-se cada letra na mensagem original por seu par. (SINGH, 2001, p. 25)

Portanto, a técnica consistia em embaralhar sem padrão determinado, de forma bijetiva as letras do alfabeto, conforme podemos ilustrar abaixo.

Exemplo 16.

A	D	H	I	K	M	O	R	S	U	W	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
V	X	B	G	J	C	Q	L	N	E	F	P	T

Ao invés de escrever ***Será esta noite*** a remetente escreveria ***NULV UNZV SQGZU***. O destinatário precisará ter acesso a chave, que é a tabela de ligação bijetiva.

Enquanto a transposição faz com que cada letra mantenha sua identidade, mas muda sua posição, na substituição as letras mudam de identidade, retendo a posição.

Todavia, o exemplo antigo mais notável de cifra de substituição é a Cifra de César. Ela foi usada para propósito militares por Júlio César nas Guerras das Gália. Nesta

ocasião foi feita uma substituição por letras do alfabeto romano pelo grego. Entretanto, encontra-se na obra *As vidas dos Césares* escrito no século II por Suetônio um processo diferente, que consistia em substituir cada letra da mensagem por outra 3 casas a frente no alfabeto. Para facilitar o processo de escrita era produzido um alfabeto cifrado, guiando as substituições como no exemplo do *Kama-sutra*. Abaixo temos um exemplo da tabela de encriptação e de uma mensagem encriptada.

Alfabeto original:

a b c d e f g h i j k l m n o p q r s t u v w x y z

Alfabeto cifrado:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Texto original: veni, vidi, vici
Texto cifrado: YHQL, YLGL, YLFL

Fonte: Reproduzida do texto Singh (2001).

Suetônio faz referencia apenas a chave 3, ou seja, que o processo de encriptação de César pulava 3 casas no alfabeto. Entretanto, podemos imaginar que outras chaves poderiam ser usadas e, considerado um alfabeto de 26 letras, existem 26 possibilidades de encriptação usando o algorítimo da Cifra de César. Isso é o suficiente para se concluir que não se tratava de um processo de embaralhamento muito seguro pois, para o oponente, conhecendo (ou suspeitando) ele o algoritmo, bastava tentar 26 chaves distintas. Por outro lado, se fizermos uma variação no algoritmo, de modo que a construção do algorítmo seja aleatória e a chave consista no alfabeto cifrado fixado, então o número de permutações possíveis para o nosso alfabeto com 26 letras distintas é dado por:

$$26! = 26 \times 25 \times 24 \times \cdots \times 2 \times 1 = 403\,291\,461\,126\,605\,635\,584\,000\,000,$$

ou seja,

$$26! \approx 4{,}03 \times 10^{26}.$$

Abaixo segue um exemplo de um processo de encriptação semelhante ao de César, mas com algoritmo aleatório. Esse alfabeto encriptado é uma das $4{,}03 \times 10^{26}$ possibilidades.

Alfabeto original:

a b c d e f g h i j k l m n o p q r s t u v w x y z

Alfabeto cifrado:

J L P A W I Q B C T R Z Y D S K E G F X H U O N V M

Texto original: et tu, bruté?
Texto cifrado: WX XH, LGHXW?

Fonte: Reproduzida do texto Singh (2001)

Uma forma de criar um padrão - ou chave - para esse embaralhamento a fim de facilitar o o processo de desencriptação com o remetente é escolher um apalavra, retirar as letras repetidas e fixa-las como o princípio do alfabeto. Por exemplo, tomemos como frase-chave **JULIUS CÉSAR**, removendo as letras repetidas e os espaços, fica **JULISCAER**. Logo, essas serão as letras iniciar do alfabeto cifrado e as seguintes prosseguirão em ordem alfabética. Para aumentar a segurança, basta usar uma frase-chave maior, o que reduz a quantidade de palavras em ordem alfabética. A seguir, temos o alfabeto cifrado com o exemplo acima.

Alfabeto original:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabeto cifrado:	J U L I S C A E R T V W X Y Z B D F G H K M N O P Q

Fonte: Reproduzida do texto Singh (2001).

4.3 Aplicações Criptográficas do Produto de Hadamard

Após a apresentação histórica e conceitual dos fundamentos da criptografia, abordamos nesta seção uma aplicação inovadora do Produto de Hadamard no desenvolvimento de esquemas de autenticação gráfica. A proposta, baseada em quadrados latinos e nas propriedades de quasigrupos, demonstra como ferramentas da álgebra podem ser utilizadas para criptografar imagens — desde as mais simples, como a letra T formada por 5 pixels, até as mais complexas, bastando, para isso, o acréscimo de poder computacional.

O sistema de encriptação de imagem apresentado neste trabalho é baseado no artigo de Falcón et al. (2023). Antes, faz-se necessário estabelecer algumas definições.

4.3.1 Quadrados Latinos e Quasigrupos

Definição 4.1. *Um quasigrupo $(Q, *)$ é um conjunto não vazio Q com uma operação binária $* : Q \times Q \to Q$ tal que, dados quaisquer $a, b \in Q$, existem elementos únicos*

$x, y \in Q$ que satisfazem:

$$a * x = b \quad e \quad y * a = b.$$

O conceito de quadrado latino é bem antigo e de fácil compreensão. Segundo Dénes e Keedwell (1991):

> Um *quadrado latino* foi considerado por Euler como uma matriz quadrada com n^2 entradas, utilizando n elementos distintos, de modo que nenhum deles se repita em qualquer linha ou coluna da matriz. O inteiro n é chamado de *ordem* do quadrado latino. (Quando conveniente, assumiremos que os elementos do quadrado latino são os inteiros $0, 1, \ldots, n-1$ ou, alternativamente, $1, 2, \ldots, n$, sem que isso implique qualquer perda de generalidade.) (DéNES; KEEDWELL, 1991)

Assim, faremos a seguinte definição foral para quadrado latino:

Definição 4.2. *Sejam S um conjunto de n símbolos distintos e $L = [l_{ij}]$ uma matriz de ordem n, onde $l_{ij} \in S$. Dizemos que L é um quadrado latino se, para todo $i, j \in \{1, 2, \ldots, n\}$:*

- *Cada linha de L contém todos os elementos de S sem repetições;*
- *Cada coluna de L contém todos os elementos de S sem repetições.*

Exemplo 17. Considere o conjunto $Q = \{1, 2, 3\}$ e a seguinte tabela de operação binária $*$:

$*$	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

Essa tabela define uma operação binária sobre Q que satisfaz a propriedade de existência e unicidade de soluções para $a * x = b$ e $y * a = b$, para todos $a, b \in Q$. Assim, $(Q, *)$ é um quasigrupo.

Além disso, a tabela acima também é um quadrado latino, pois cada símbolo do conjunto Q aparece exatamente uma vez em cada linha e em cada coluna.

Exemplo 18. Considere agora o conjunto $Q = \{a, b, c, d\}$ com a seguinte tabela de operação:

$*$	a	b	c	d
a	b	a	d	c
b	c	d	a	b
c	d	c	b	a
d	a	b	c	d

Essa operação também define um quasigrupo, e a tabela é um quadrado latino de ordem 4, pois cada símbolo aparece exatamente uma vez em cada linha e coluna.

Esses não são casos especiais, todo quasigrupo finito pode ser representado por um quadrado latino, usando sua tabela de multiplicação. Este é o primeiro teorema trazido no livro de Dénes e Keedwell (1991), que apresentaremos a seguir.

Teorema 4.1. *Toda tabela de multiplicação de um quasigrupo é um quadrado latino e, inversamente, todo quadrado latino com borda é a tabela de multiplicação de um quasigrupo.*

Demonstração. Sejam $a_1, a_2, \ldots, a_n$ os elementos do quasigrupo e seja sua tabela de multiplicação conforme ilustrado na tabela 4.3.1, onde o elemento a_{rs} que aparece na linha r e coluna s é o produto $a_r a_s$ dos elementos a_r e a_s.

	a_1	a_2	$\cdots$	a_r	$\cdots$ a_s	$\cdots$	a_n
a_1	a_{11}				$\vdots$		$\vdots$
a_2					$\vdots$		$\vdots$
$\vdots$					$\vdots$		$\vdots$
a_r	$\cdots$	$\cdots$	$\cdots$	$\cdots$	a_{rs}		$\vdots$
$\vdots$							$\vdots$
a_n	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	a_{nn}

Tabela 1 – Tabela de multiplicação de um quasigrupo.

Se algum elemento aparecesse duas vezes na linha r, digamos nas colunas s e t, então teríamos $a_{rs} = a_{rt} = b$, o que implicaria duas soluções para a equação $a_r x = b$, contrariando os axiomas do quasigrupo. De modo semelhante, se o mesmo elemento ocorresse duas vezes na coluna s, teríamos duas soluções para a equação $y a_s = c$, para algum c.

Concluímos, portanto, que cada elemento do quasigrupo aparece exatamente uma vez em cada linha e uma vez em cada coluna, e assim a tabela de multiplicação sem bordas (que é uma matriz quadrada de n linhas e n colunas) é um quadrado latino. ■

4.3.2 Esquema de senha gráfica baseado em quadrados latinos

Um dos elementos centrais do sistema criptográfico que trabalharemos nesta seção é o quadrado latino que está definido em $\mathbb{N} = \{1, 2, \ldots, n\}$. O Produto de Hadamard

entra nesse sistema como um distribuidor de multiplicação, associado ao quadrado latino L.

Definição 4.3. *Sejam $A = [a_{ij}], B = [b_{ij}] \in M_n(\mathbb{N})$ e seja L um quadrado latino de ordem $q = \max\{a_{ij},\ b_{ij}\}$. Define-se a operação*

$$(A \circledast_L B)[i,j] = L[A[i,j], B[i,j]], \tag{4.2}$$

onde $L[a,b]$ representa a entrada da matriz L localizada na linha a e coluna b. Além disso, $A[i,j]$ e $B[i,j]$ denotam, respectivamente, os elementos das matrizes A e B na linha i e coluna j, com $i, j \in \mathbb{N}$.

Exemplo 19. Sejam as matrizes:

$$A = \begin{bmatrix} 2 & 2 & 3 \\ 3 & 1 & 2 \\ 1 & 3 & 3 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 3 & 2 \\ 3 & 2 & 3 \\ 2 & 2 & 1 \end{bmatrix} \text{ e } \quad L = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}.$$

O produto $A \circledast_L B$ resulta em:

$$A \circledast_L B = \begin{bmatrix} L[2,1] & L[2,3] & L[3,2] \\ L[3,3] & L[1,2] & L[2,3] \\ L[1,2] & L[3,2] & L[3,1] \end{bmatrix} = \begin{bmatrix} 2 & 1 & 1 \\ 2 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix}.$$

Basicamente, os valores de A e B serão usados como coordenadas para buscar os valores da operação em L.

Um sistema criptográfico eficiente é aquele em que a mensagem, após encriptada, poderá sempre voltar a sua forma original. O que garante a eficiência do sistema aqui apresentado é o teorema a seguir. A demonstração foge do escopo de nosso trabalho, mas poderá ser consultada em Falcón et al. (2023).

Teorema 4.2. *Para todo A então existe um ρ tal que:*

$$A \circledast_L^{\rho} L = A$$

ou seja, o produto iterado pode recuperar a matriz original.

Exemplo 20. Seja M a matriz mensagem e K a matriz chave definidas da seguinte maneira:

$$M = \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix}, \qquad K = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}.$$

Logo, por M e K possuírem entradas naturais em $\{1, 2, 3\}$, então o quadrado latido necessário para aplicação do sistema de encriptação deverá ser de ordem 3. Portanto, seja L o seguinte quadrado latino:

$$L = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}.$$

O Produto de Hadamard sobre L será:

$$\begin{aligned} C = M \odot_L K &= \begin{bmatrix} L[m_{11}, k_{11}] & L[m_{12}, k_{12}] \\ L[m_{21}, k_{21}] & L[m_{22}, k_{22}] \end{bmatrix} \\ &= \begin{bmatrix} L[1,2] & L[3,1] \\ L[2,3] & L[2,2] \end{bmatrix} \\ &= \begin{bmatrix} 2 & 3 \\ 1 & 3 \end{bmatrix}. \end{aligned}$$

Assim, dado o criptograma C, a chave K e o quadrado latino L, buscamos o valor de cada m_{ij} que satisfaz $L[m_{ij}, k_{ij}] = c_{ij}$.

- m_{11} – Temos $c_{11} = L[m_{11}, 2] = 2$, então, ao olhar o quadrado latino L na coluna 2, percebemos que o valor 2 aparece apenas na linha 1. Portanto, $m_{11} = 1$.
- m_{12} – Temos $c_{12} = L[m_{12}, 1] = 3$, então, ao analisar a coluna 1 do quadrado latino L, vemos que o valor 3 ocorre somente na linha 3. Logo, $m_{12} = 3$.
- m_{21} – Temos $c_{21} = L[m_{21}, 3] = 1$, então, observando a coluna 3 do quadrado latino L, notamos que o valor 1 aparece apenas na linha 2. Assim, $m_{21} = 2$.
- m_{22} – Temos $c_{22} = L[m_{22}, 2] = 3$, então, olhando a coluna 2 de L, percebemos que o número 3 surge unicamente na linha 2. Portanto, $m_{22} = 2$.

Portanto, recuperamos a matriz original:

$$M = \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix}.$$

Observações finais:

- O uso de um quadrado latino garante que cada par (m_{ij}, k_{ij}) gere um valor único e reversível.
- A segurança depende do sigilo da chave K, não necessariamente de L.
- Para manter o sistema válido, todos os valores de M e K devem ser números naturais entre 1 e a ordem de L.

4.4 Considerações finais

Este exemplo mostra claramente como estruturas matemáticas, como quadrados latinos e produtos matriciais, podem ser utilizadas de forma criativa em aplicações de segurança digital. O Produto de Hadamard, neste contexto, serve como uma ferramenta criptográfica poderosa, operando como um operador de transformação segura que se encaixa naturalmente em esquemas de autenticação gráfica.

5 Aplicações Didáticas

5.1 Introdução

Neste capítulo, propomos um conjunto de atividades envolvendo criptografia e criptoanálise, voltadas para aplicação no Ensino Básico. As propostas têm como objetivo integrar conteúdos matemáticos previamente abordados, adaptando-os aos diferentes contextos e faixas etárias encontradas no Ensino Fundamental II e no Ensino Médio.

A criptografia, aliada à criptoanálise, configura-se como um tema altamente motivador para a introdução e aprofundamento de diversos conteúdos matemáticos, como permutação, propriedades geométricas (como as do cilindro), matrizes e operações inversas. O caráter enigmático e investigativo dessas práticas favorece o engajamento dos estudantes em atividades desafiadoras e criativas.

5.1.1 Motivação: linguagem, curiosidade e o desejo de compartilhar segredos

Utilizar jogos, dinâmicas e contextualização vem se tornando um dos principais temas sobre ensino de Matemática nos últimos anos. O que se pretende é dar mais sentido e trazer mais interesse à área, em especial para os estudantes de menor idade. Com isso em mente, foi pensado em quais atividades e temas poderiam ter elevado potencial de engajamento entre alunos, em especial aqueles entre 11 e 17 anos de idade, presentes em sua maioria no Ensino Fundamental II e Médio. Estudar as origens da criptografia nos possibilitou entender o interesse humano por trás dela, o que está intimamente ligado à necessidade que possibilitou à nossa espécie desenvolver a fala. É por esse motivo que parte considerável das atividades propostas neste capítulo consiste em utilizar a função nativa da criptografia: a ocultação de mensagens.

Uma interessante explanação da vantagem obtida, direcionador do nosso sistema evolutivo, foi feita por Harari (2015) no Capítulo 2, onde o autor aborda a Revolução Cognitiva. As informações sobre o processo evolutivo humanos contidas neste capítulo são todas retiradas desta obra.

Hoje a única espécie humana existente é o *Homo sapiens*, entretanto, nem sempre foi assim. Por volta de 150 mil anos atrás, o planeta Terra era habitado simultaneamente por *sapiens* e *neandertais*. Há registro de conflito entre essas duas espécies há 100 mil anos, em que os *neandertais* saíram vencedores. Entretanto, por volta de 70 mil anos atrás, uma revolução ocorreu em nossa espécie: a Revolução Cognitiva. Embora *sapiens* primitivos tivessem uma estrutura corporal muito próxima da nossa, sua ca-

pacidade cognitiva era muito inferior. O processo evolutivo possibilitou que esses seres desenvolvessem habilidades que os tornaram tão poderosos a ponto de extinguirem da face da Terra todas as outras espécies humanas.

O que diferenciou os *sapiens* foi sua notável habilidade de colaborar em larga escala, inclusive com indivíduos desconhecidos. Essa capacidade de formar redes de confiança e cooperação com base em mitos compartilhados, sistemas simbólicos e linguagem complexa é o que fundamenta as estruturas sociais humanas até hoje. É o que permite, por exemplo, que pais deixem seus filhos com professores desconhecidos ou que pessoas comprem alimentos produzidos por indivíduos que jamais conheceram.

Uma das principais engrenagens na construção desse ecossistema de cooperação é nossa capacidade de nos comunicar de forma complexa. Não se trata do primeiro sistema de comunicação — todos os animais, de alguma forma, possuem algum sistema de comunicação, até mesmo insetos. Experimentos realizados em zoológicos identificaram sons característicos usados por macacos-verdes para indicar leões — fazendo com que eles se escondessem nas árvores — e outro som para águias — fazendo com que saíssem de campo aberto. A diferença está no nível de detalhes que nosso sistema de comunicação oferece. Qual vantagem favoreceu o surgimento de nosso sistema de comunicação? Algumas linhas de pesquisa apontam que nossa linguagem evoluiu como instrumento para troca de fofocas. Isso por ser o *Homo sapiens* um animal altamente sociável. "Não basta que determinados homens e mulheres saibam onde se encontram os leões e os bisões. É muito mais relevante para eles saber quem no grupo odeia quem, quem está dormindo com quem, quem é honesto, quem é trapaceiro." (HARARI, 2015) Em sociedades tribais, saber quem está com quem, quem é confiável ou quem representa uma ameaça social era tão ou mais importante do que saber onde havia alimento ou predadores.

É nesse ponto que a criptografia ganha um novo sentido pedagógico. Aprender matemática requer esforço e concentração; por outro lado, compartilhar segredos — ou "fofocar" — é uma prática instintiva, envolvente e emocionalmente carregada. Unir essas duas dimensões pode gerar um ambiente de aprendizagem extremamente produtivo. Ao apresentar aos estudantes a proposta de codificar mensagens secretas para colegas, introduzimos uma narrativa lúdica e instigante que os convida a desvendar mistérios — e, nesse processo, desenvolver competências matemáticas significativas. Evidentemente, é fundamental que a prática venha acompanhada de discussões éticas, mas o simples anúncio de que a aula do dia ensinará como escrever mensagens secretas, talvez codificar um segredo para um amigo, já tem o potencial de acender a curiosidade e o entusiasmo dos alunos.

5.2 Fundamentação Didática

Neste tópico, discutimos os fundamentos pedagógicos que sustentam a proposta de atividades com criptografia no ensino básico. Apresentamos uma abordagem teórica sobre o ensino de álgebra e matrizes, as competências da BNCC envolvidas e o potencial da criptografia como recurso pedagógico.

5.2.1 Abordagem teórica sobre o ensino de álgebra e matrizes no Ensino Fundamental II e Médio

O ensino de álgebra no Ensino Fundamental II marca a transição do pensamento aritmético para o pensamento algébrico, desenvolvendo a capacidade de generalização, abstração e formalização dos estudantes. Segundo Campos e Farias (2020):

> Propor atividades aritméticas e algébricas na forma de resolução de problemas é um caminho para o desenvolvimento do pensamento algébrico, pelas relações e conexões que necessita estabelecer para a solucioná-los. O uso da linguagem natural e de situações contextualizadas nos problemas matemáticos aproxima o aluno de sua realidade, do que lhe é próximo, útil e prazeroso, além de desmistificar a ideia de uma disciplina de difícil aprendizagem. (CAMPOS; FARIAS, 2020, p. 177)

Para os autores, contextualizar é trazer sentido ao que se ensina, em Matemática, é um facilitador do aprendizado. Tornar a disciplina mais significativa e atrativa é fundamental para a expansão do aprendizado. Da mesma forma, a abordagem de matrizes no Ensino Médio representa uma oportunidade de ampliar a compreensão dos estudantes sobre representações matemáticas e operações entre objetos não numéricos.

A Proposta Curricular do Ensino Médio da Paraíba segue as diretrizes da Base Nacional Comum Curricular (BNCC), que estabelece a Formação Geral Básica (FGB) como componente obrigatório para todos os estudantes do Ensino Médio. Dentro dessa formação, a habilidade EM13MAT410 destaca-se ao associar o conceito de matrizes, determinantes e sistemas de equações lineares às situações nas quais são utilizadas planilhas eletrônicas (Secretaria da Educação do Estado da Paraíba, 2023).

Mesmo não tendo a BNCC detalhado explicitamente o ensino tradicional de operações com matrizes e determinantes, a inclusão desses conceitos na habilidade EM13MAT410 da Proposta Curricular do Ensino Médio da Paraíba implica que os estudantes devem:

- Compreender a estrutura e a função das matrizes e determinantes;
- Aplicar esses conceitos na resolução de sistemas de equações lineares;

- Utilizar planilhas eletrônicas como ferramenta para representar e resolver problemas envolvendo esses tópicos.

Além disso, Freudenthal (1994), descreve um processo ao qual decidiu chamar de Educação Matemática Realística (RME), onde se propõe uma abordagem inovadora para o ensino da Matemática, centrada na ideia de que a Matemática deve ser compreendida como uma atividade humana. Para Freudenthal, os alunos não devem apenas receber conhecimentos matemáticos prontos, mas sim serem incentivados a reinventá-los, redescobrindo conceitos a partir de situações significativas.

Na perspectiva da RME, o termo "realística" refere-se não apenas a situações do mundo real, mas a qualquer contexto que seja significativo para o aluno. Isso inclui contextos do cotidiano, de jogos, histórias ou situações imaginárias — desde que façam sentido para os estudantes. Assim, a aprendizagem Matemática passa a ser construída a partir de experiências contextualizadas, possibilitando o desenvolvimento do raciocínio matemático com base na realidade vivida ou compreendida pelos alunos.

Assim, a Matemática não deveria ser imposta aos estudantes sem antes passar pelo processo de experimentação e vivência de seus conceitos. Nesse sentido, o uso da criptografia como tema gerador oferece um espaço autêntico para mobilizar noções matemáticas em contextos problematizadores, nos quais o estudante reconhece a funcionalidade do conteúdo.

5.2.2 Referências à BNCC: competências gerais e específicas de Matemática

A Base Nacional Comum Curricular (2018) orienta que o ensino de Matemática deve ir além do domínio de algoritmos e procedimentos, sendo responsável pela formação de sujeitos críticos, criativos e autônomos. Nesse sentido, o uso da criptografia dialoga diretamente com várias competências gerais da BNCC, sendo elas:

> 1. Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva. [...] 4. Utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital –, bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos e produzir sentidos que levem ao entendimento mútuo. (Base Nacional Comum Curricular, 2018)

Além das competências gerais, dentro das atividades criadas posteriormente neste capítulo, conectamos diversas habilidades da Base Nacional Comum Curricular (2018), essenciais para o desenvolvimento do alunado. Por vezes, as atividades trabalham

habilidades que dizem respeito tanto aos alunos do Ensino Fundamental – anos finais – quanto aos do Ensino Médio.

Sendo assim, os diversos sistemas de criptografia apresentados neste trabalho e abordados neste capítulo podem ser considerados elos de ligação entre o mundo abstrato da Matemática e as realidades do cotidiano humano, além de conferirem sentido a múltiplos entes teóricos matemáticos.

Além disso, podemos destacar como esse tema se conecta com Ministério da Educação (Brasil) (2022), documento complementar à BNCC que trata da Computação na Educação Básica. Para o 9º ano, destaca-se a habilidade EF09CO05, que consiste em "analisar técnicas de criptografia para armazenamento e transmissão de dados".

O documento apresenta os seguintes exemplos de aplicação dessa habilidade em sala de aula:

> (1) Apresentando o conceito de criptografia, por exemplo, usando algoritmos simples de criptografia para que os estudantes codifiquem textos e frases e troquem mensagens criptografadas com os colegas. (2) Discutindo a importância do tráfego de informações criptografadas nas redes, por exemplo, em relação a dados como senhas e informações bancárias das pessoas. (3) Discutindo o papel histórico da criptografia, por exemplo, na comunicação de informações sigilosas durante a Segunda Guerra Mundial.(Ministério da Educação (Brasil), 2022)

Portanto, as práticas aqui apresentadas podem ser uma importante ferramenta de materialização do que a BNCC propõe para a educação básica.

5.2.3 O potencial da criptografia como tema gerador ou prática de modelagem Matemática

A criptografia pode ser entendida como um *tema gerador* freireano, pois está enraizada em uma prática social concreta e desperta o interesse espontâneo dos alunos. Sua utilização didática permite abordar não apenas conteúdos matemáticos específicos, mas também desenvolver uma postura investigativa e reflexiva sobre a informação, a privacidade e a comunicação. Segundo Freire (1987), o tema gerador nasce da realidade vivida e é potente por permitir a problematização do cotidiano do educando.

Por outro lado, a criptografia também pode ser concebida como uma prática de *modelagem Matemática*, ao exigir que o aluno construa representações e algoritmos para resolver problemas contextualizados. No processo de criar, codificar e decodificar mensagens, o estudante realiza a modelagem de situações reais por meio de operações, equações, funções e matrizes. Isso cria uma ponte direta entre a matemática escolar e sua aplicabilidade no mundo real e digital.

Para Bassanezi (2002, p. 16), modelagem Matemática consiste "[...] na arte de transformar problemas da realidade em problemas matemáticos e resolvê-los, interpretando suas soluções na linguagem do mundo real". Para o autor, trata-se do elo de conexão entre teoria e prática, fundamental na construção educacional do aluno, possibilitando que ele compreenda as teorias envolvidas nos fenômenos que o cercam, e colocando-o na posição de agente transformador.

5.3 Descrição da Proposta Educacional

A proposta educacional aqui apresentada tem como objetivo integrar conceitos matemáticos e fundamentos de criptografia por meio de uma abordagem contextualizada, interdisciplinar e investigativa.

5.3.1 Público-alvo

As atividades aqui apresentadas são direcionadas a estudantes de todo o Ensino Básico, com ressalva para as atividades 4 e 5, que envolvem matrizes e se tornam mais adequadas para alunos da segunda e terceira séries do Ensino Médio, pois é nessa fase que, segundo (Secretaria de Estado da Educação da Paraíba, 2023), tais conteúdos devem ser trabalhados. Esse público se encontra em uma etapa crucial do desenvolvimento cognitivo, apresentando maior capacidade de abstração e interesse por temas ligados à tecnologia, lógica e resolução de desafios.

Além disso, as atividades de cunho histórico apresentadas são inspiradas nas obras de Singh (2001), abordadas neste trabalho, enquanto Falcón et al. (2023) serviu de base para a atividade sobre o Produto de Hadamard.

5.3.2 Pré-requisitos necessários

Para as Atividades 1, 2 e 3, é necessário apenas que o estudante possua bom letramento. Isso porque, embora conceitos matemáticos estejam presentes em todas as atividades, elas se concentram em embaralhar letras, sem a necessidade de grandes operações. As atividades 4 e 5, por outro lado, exigem uma introdução a matrizes, ao Produto de Hadamard e domínio de operações básicas com números naturais, para encriptar e desencriptar a mensagem.

5.3.3 Metodologia utilizada

A metodologia adotada combina diferentes abordagens didáticas, com destaque para:

- **Ensino por investigação**: os alunos são convidados a explorar códigos e criar suas próprias mensagens criptografadas, promovendo descobertas por meio da análise de padrões e estruturas matemáticas.

- **Resolução de problemas**: as atividades envolvem desafios reais e históricos relacionados à criptografia, estimulando a aplicação de conteúdos matemáticos para encontrar soluções.

- **Gamificação**: é possível inserir elementos lúdicos, como "missões" secretas, desafios entre grupos ou simulações de comunicação criptografada, para aumentar o engajamento e promover a aprendizagem ativa.

Essa proposta visa desenvolver habilidades cognitivas, sociais e matemáticas, promovendo o protagonismo do estudante e o uso significativo da matemática como ferramenta para interpretar e transformar a realidade.

5.4 Atividades de Criptografia

Todas as atividades a seguir estão fundamentadas na ideia de comunicação sigilosa. Partimos da premissa de que, na história evolutiva humana, a capacidade de transmitir informações de forma reservada (o "segredo", a "fofoca" como vantagem evolutiva) foi um fator determinante para o desenvolvimento da linguagem e da organização social. Assim, convidamos os estudantes a vivenciarem a produção e decodificação de mensagens cifradas por diferentes técnicas, cada uma vinculada a um contexto histórico ou matemático específico.

5.4.1 Atividade 1 – Cifra de César: Alerta ao Aliado

Ilustração:

Figura 12 – Soldado escrevendo a mensagem criptografada

Fonte: Imagem gerada com o auxílio da inteligência artificial ChatGPT, OpenAI, em [05/2025].

Habilidades contempladas:

- (EF08MA03) Resolver e elaborar problemas de contagem cuja resolução envolva a aplicação do princípio multiplicativo.
- (EF07MA05) Resolver um mesmo problema utilizando diferentes algoritmos.
- (EM13MAT306) Resolver e elaborar problemas em contextos que envolvem fenômenos periódicos reais (ondas sonoras, fases da lua, movimentos cíclicos, entre outros) e comparar suas representações com as funções seno e cosseno, no plano cartesiano, com ou sem apoio de aplicativos de álgebra e geometria.
- (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.
- (EM13MAT507) Identificar e associar progressões aritméticas (PA) a funções afins de domínios discretos, para análise de propriedades, dedução de algumas fórmulas e resolução de problemas.

Orientações metodológicas:

- Tempo estimado: a atividade pode ser realizada em aproximadamente 50 minutos, sendo 15 minutos para introdução histórica e explicação do funcionamento da cifra, 20 minutos para os alunos codificarem e decodificarem as mensagens, e 15 minutos para socialização e discussão dos resultados. Conforme pode se constatar nas instruções a seguir, em séries mais avançadas é possível explorar ainda mais a atividade, de modo que para esses casos mais tempo pode ser demandado.

- Nível de dificuldade: trata-se de uma atividade de baixa complexidade conceitual, adequada a alunos a partir do 7º ano do Ensino Fundamental. Embora simples, ela estimula habilidades importantes como reconhecimento de padrões, pensamento algorítmico e lógica de substituição.

- Apresentar o contexto histórico da cifra de César, destacando sua aplicação na Roma Antiga como forma de comunicação militar sigilosa. Esse momento inicial pode despertar o interesse dos alunos ao evidenciar a conexão entre Matemática e História.

- Explicar o funcionamento da cifra de César, utilizando exemplos simples com palavras curtas para demonstrar como ocorre o deslocamento no alfabeto. Pode-se construir coletivamente uma tabela de substituição com diferentes valores de deslocamento, estimulando a participação ativa.

- Explorar o conceito de periodicidade e modularidade, relacionando o alfabeto ao comportamento cíclico dos números em módulos, de forma introdutória. Essa conexão ajuda a compreender a natureza matemática da cifra como uma aplicação prática da aritmética modular.

- Distribuir a atividade em grupos ou duplas, de forma que cada grupo codifique uma mensagem e a repasse a outro para decodificação. Esse formato favorece a interação, o raciocínio lógico e a verificação mútua do processo de codificação/decodificação.

- Estimular a elaboração de algoritmos, sugerindo que os alunos representem, em linguagem natural ou por fluxogramas, os passos para codificar e decodificar mensagens. Essa abordagem favorece o desenvolvimento do pensamento algorítmico, conforme previsto na BNCC.

- Promover a reflexão sobre segurança e padrões, discutindo com os alunos as limitações da cifra de César (como a vulnerabilidade à análise de frequência) e incentivando a busca por regularidades na mensagem cifrada, desenvolvendo a capacidade de observação e análise crítica.

- Relacionar a atividade a conteúdos curriculares, como sequências numéricas, padrões, regularidades, funções periódicas e princípios de contagem, conforme o nível da turma, valorizando a interdisciplinaridade e a aplicabilidade da Matemática.

Objetivo: Compreender a ideia de substituição e deslocamento no alfabeto, além de exercitar o reconhecimento de padrões e desenvolver atenção à linguagem escrita.

Por exemplo, ao mudar o padrão de deslocamento, digamos para 5, a letra mais frequente na mensagem cifrada por ser um representante da letra “a”, entregando o segredo da encriptação.

Enunciado: Seu grupo faz parte de uma resistência secreta. Você precisa enviar um bilhete para avisar seus aliados de que `O INIMIGO CHEGARÁ À MEIA-NOITE`. Use a cifra de César com deslocamento de 3 letras para codificar a mensagem. Escreva a mensagem cifrada no papel e entregue a um colega que será o responsável por decifrá-la.

Alfabeto original: ↓

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Alfabeto cifrado (deslocamento +3): ↑

Mensagem cifrada: `R LQLPLJR FKHJDUÁ À PHLD-QRLWH`

Avaliação:

- Aplicação correta do deslocamento no alfabeto: o professor deverá conferir se os alunos conseguiram codificar corretamente a mensagem, utilizando o deslocamento de três letras conforme indicado. Isso demonstra a compreensão do funcionamento da cifra.

- Reconhecimento de padrões e regularidades: ao analisar a mensagem cifrada produzida pelos alunos, o professor poderá avaliar se eles compreenderam a lógica da substituição e identificaram a regularidade envolvida no processo de encriptação.

- Interpretação e decodificação: caso a atividade seja realizada em duplas ou grupos (com um aluno decodificando a mensagem do outro), o professor poderá verificar se o aluno que recebe a mensagem é capaz de aplicar o processo inverso, ou seja, decifrar corretamente o conteúdo, evidenciando domínio do mecanismo de substituição.

5.4.2 Atividade 2 – Cítale Espartano: O dia do amigo

Instrução visual:

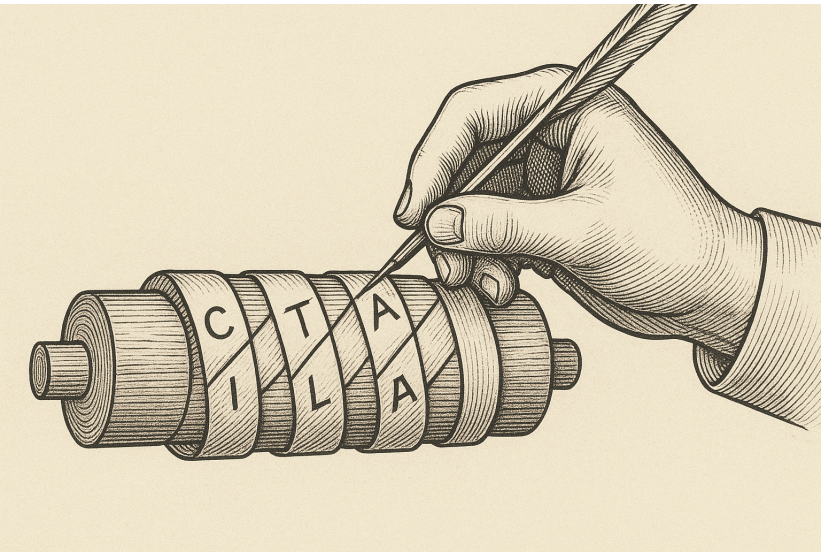


Figura 13 – Exemplificação de construção do Cítale Espartano

Fonte: Imagem gerada com o auxílio da inteligência artificial ChatGPT, OpenAI, em [05/2025].

Habilidades contempladas:

- (EF09MA19) Resolver e elaborar problemas que envolvam medidas de volumes de prismas e de cilindros retos, inclusive com uso de expressões de cálculo, em situações cotidianas.
- (EF08MA19) Resolver e elaborar problemas que envolvam medidas de área de figuras geométricas, utilizando expressões de cálculo de área (quadriláteros, triângulos e círculos), em situações como determinar medida de terrenos.
- (EM13MAT201) Propor ou participar de ações adequadas às demandas da região, preferencialmente para sua comunidade, envolvendo medições e cálculos de perímetro, de área, de volume, de capacidade ou de massa.
- (EM13MAT309) Resolver e elaborar problemas que envolvem o cálculo de áreas totais e de volumes de prismas, pirâmides e corpos redondos em situações reais (como o cálculo do gasto de material para revestimento ou pinturas de objetos cujos formatos sejam composições dos sólidos estudados), com ou sem apoio de tecnologias digitais.
- (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.
- (EM13MAT504) Investigar processos de obtenção da medida do volume de prismas, pirâmides, cilindros e cones, incluindo o princípio de Cavalieri, para a obtenção das fórmulas de cálculo da medida do volume dessas figuras.

Orientações metodológicas:

- Tempo estimado: a atividade pode ser desenvolvida em 1 ou 2 aulas (50 a 100 minutos), a depender da disponibilidade de materiais e da etapa escolar. A primeira aula pode ser dedicada à construção do *cítale* e à escrita da mensagem, e a segunda, à leitura cruzada, discussão dos resultados e sistematização dos conceitos geométricos.

- Nível de dificuldade: atividade de baixa a média complexidade, adequada para turmas a partir do 6º ano do Ensino Fundamental.

- Contextualização histórica: inicie a aula apresentando brevemente o uso do *cítale* na Grécia Antiga como instrumento militar de codificação. Mostre como a matemática, desde tempos antigos, esteve envolvida com segurança da informação, promovendo uma abordagem interdisciplinar com História.

- Exploração geométrica: para alunos a partir do 8º ano do Ensino Fundamental, discuta as propriedades do cilindro que influenciam o sucesso da decodificação da mensagem, como o perímetro da base, a altura da tira de papel e a área da superfície lateral. Estimule os alunos a calcularem essas medidas e a testarem *citales* com diâmetros diferentes para observar os efeitos na leitura da mensagem.

- Deve-se enrolar a tira no *Cítale* de forma justa para que se possa fazer a encriptação perfeitamente.

- Organização da turma: os alunos podem trabalhar em duplas ou grupos. Cada grupo constrói um *cítale* e codifica uma mensagem que será entregue a outro grupo, o qual tentará decodificá-la utilizando o seu próprio cilindro. Essa troca permite que descubram, na prática, o papel do diâmetro como "chave".

- Discussão e sistematização: ao final, promova uma roda de conversa para que os alunos compartilhem o que observaram ao tentar decodificar mensagens com cilindros de diâmetros diferentes. Esse momento favorece a abstração dos conceitos geométricos envolvidos e reforça a noção de codificação e chave.

- Integração com conteúdos curriculares: a atividade favorece a abordagem de conteúdos como perímetro, área, volume, medidas não convencionais e propriedades do cilindro. Além disso, permite a articulação com temas da Base Nacional Comum Curricular (2018) como resolução de problemas, pensamento algorítmico e argumentação.

Objetivo geral: Aplicar o conceito histórico de criptografia por transposição, compreendendo a importância do diâmetro do cilindro como chave. O *citale* pode ser usado como elemento motivador para o estudo das propriedades do cilindro.

Contexto histórico: Na Grécia antiga, militares espartanos enviavam mensagens codificadas usando uma tira de couro enrolada num bastão. Apenas quem possuía um bastão com o mesmo diâmetro conseguia ler corretamente.

Materiais: Tiras de papel (3–4 cm de altura), canetas e cilindro oco (garrafa, cano, rolo de papel, etc).

Atividade:

1. Ornamente o cilindro para que se torne uma embalagem atrativa;

2. Enrole a tira no cilindro e escreva a mensagem horizontalmente;

3. Desenrole: o texto parecerá embaralhado;

4. Guarde a mensagem dentro do cilindro e presenteie a pessoa desejada.

Objetivo específico: O aluno produzirá uma embalagem cilíndrica que terá duas funções: guardar a mensagem em seu interior e decodificá-la, quando a tira de texto for enrolada na própria embalagem. A ideia, neste caso, é que terceiros, ao terem acesso à carta, não consigam compreendê-la, caso desconheçam o funcionamento do sistema de encriptação. Não se pretende criar uma encriptação com elevado teor de segurança, visto que o cítale estará junto da mensagem. Para este caso, pretende-se criar um souvenir que permita usar a matemática de maneira prática, lúdica e atrativa, permitindo ao aluno, além de criar objetos de arte, estimulando a sua criatividade, fazendo uso do pensamento matemático para resolução de problemas.

Avaliação:

- Compreensão do sistema criptográfico: Verifica-se se o aluno compreendeu o princípio de funcionamento do *citale* espartano, identificando que o diâmetro do cilindro funciona como a chave da transposição. Incentivá-los a conectar suas tiras de mensagens nos diferentes *citales* dos colegas pode ser elemento motivador desse descobrimento.

- Aplicação de conhecimentos geométricos: Avalia-se se o aluno foi capaz de aplicar corretamente conceitos de geometria, como medidas de área da tira de papel, perímetro da base e superfície lateral do cilindro utilizado. Essa análise pode ocorrer durante a construção da embalagem e o processo de enrolar a tira.

- Verificação de exercícios referente a propriedades dos cilindros.

5.4.3 Atividade 3 – Trilho de Trem: A mensagem da resistência

Ilustração:

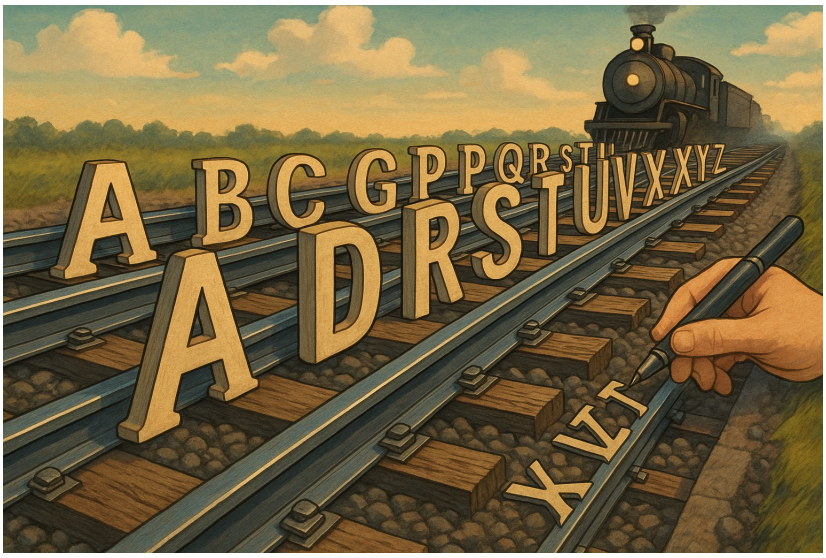


Figura 14 – Trilho da criptografia

Fonte: Imagem gerada com o auxílio da inteligência artificial ChatGPT, OpenAI, em [05/2025].

Habilidades contempladas:

- (EF07MA05) Resolver um mesmo problema utilizando diferentes algoritmos.
- (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.

Orientações metodológicas:

- Tempo estimado: recomenda-se dedicar 20 minutos para a introdução e outros 20 minutos para a realização da atividade. Caso o professor deseje promover uma discussão mais aprofundada sobre diferentes algoritmos de codificação, uma aula adicional pode ser utilizada para análise comparativa entre cifras.
- Nível de dificuldade: a atividade possui dificuldade baixa. Pode ser aplicada a partir do 6º ano do Ensino Fundamental, sendo também adequada ao Ensino Médio, sobretudo como introdução ao pensamento algorítmico e à noção de padrões.

- Estratégia de ensino: inicie a aula explicando o funcionamento da cifra de trilho de trem e faça um exemplo coletivo com a turma no quadro. Em seguida, proponha que os alunos desenvolvam suas próprias mensagens com dois ou três trilhos, testando diferentes configurações.

- Organização da turma: recomenda-se o trabalho em duplas ou pequenos grupos. Após a criação da mensagem cifrada, cada grupo entrega sua versão a outro grupo, juntamente com pistas. Isso estimula a comunicação, a dedução lógica e o trabalho cooperativo.

- Potencial interdisciplinar: a atividade permite conexão com temas de História, ao abordar contextos de guerra e espionagem, e com Tecnologias, ao relacionar a lógica de codificação com princípios de programação, criptografia e segurança da informação.

- Ampliação da atividade: os alunos podem registrar o processo utilizado em um fluxograma, contribuindo para o desenvolvimento do pensamento computacional. Se possível, o professor pode propor o uso de planilhas ou aplicativos para automatizar a codificação.

- Encerramento e sistematização: ao final da aula, promova uma socialização dos métodos criados pelos grupos e das dificuldades enfrentadas na decodificação. Esse momento é fundamental para consolidar a compreensão da estrutura do algoritmo de transposição.

Objetivo: Introduzir a cifra de transposição por trilho de trem (Rail Fence Cipher), entendendo como o padrão de leitura altera o sentido da mensagem.

Contexto: Membros da resistência trocam mensagens embaralhadas simulando trilhos de trem para evitar a interceptação.

Exemplo: Mensagem clara:

`O ATAQUE SERÁ ÀS SEIS HORAS`

Codificação com 2 trilhos:

- Linha 1: `O T Q E E Á S E S O A`
- Linha 2: `A A U S R À S I H R S`

Resultado: `OTQEEÀSESOAAAUSRÀSIHRS`

Atividade:

1. Codifiquem mensagens com 2 ou 3 trilhos.
2. Troquem com outro grupo e deem pistas para que possam decodificar.

Avaliação:

- Compreensão do algoritmo de transposição: O professor deve verificar se o aluno compreendeu a lógica da cifra por trilho de trem, ou seja, como a reorganização das letras em linhas (trilhos) altera a leitura da mensagem. Essa compreensão pode ser observada tanto na criação da mensagem cifrada quanto na tentativa de decodificação.
- Aplicação correta da codificação: Avalia-se se o aluno consegue organizar adequadamente os caracteres da mensagem entre os trilhos (com 2 ou 3 níveis), seguindo o padrão da cifra, e gerar uma sequência final coerente com o método.
- Decodificação com base em pistas: O professor pode avaliar a capacidade do aluno de reconstruir a mensagem original a partir de uma versão cifrada recebida de outro grupo, com base nas pistas fornecidas, demonstrando raciocínio lógico e interpretação de padrões.

5.4.4 Atividade 4 – Produto de Hadamard: A primeira letra de alguém muito especial

Ilustração:

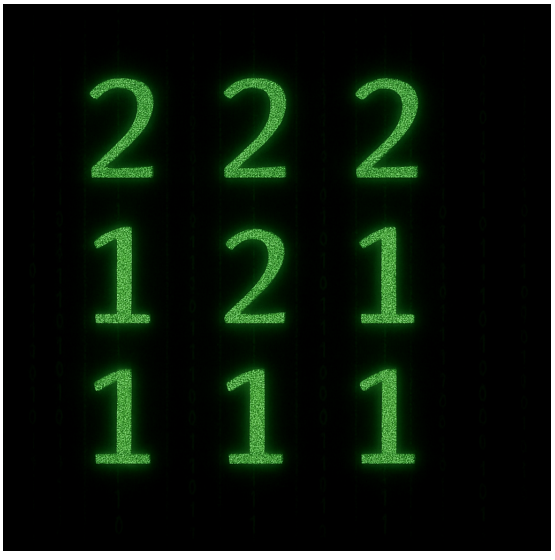


Figura 15 – "MatriX"

Fonte: Imagem gerada com o auxílio da inteligência artificial ChatGPT, OpenAI, em [05/2025].

Habilidades contempladas:

- (EF07MA05) Resolver um mesmo problema utilizando diferentes algoritmos.
- (EM13MAT203) Aplicar conceitos matemáticos no planejamento, na execução e na análise de ações envolvendo a utilização de aplicativos e a criação de planilhas (para o controle de orçamento familiar, simuladores de cálculos de juros simples e compostos, entre outros), para tomar decisões.
- (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.
- (EM13MAT405) Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática

Orientações metodológicas:

- Tempo estimado: devido ao grau de abstração e à necessidade de compreensão prévia do Produto de Hadamard e de matrizes, recomenda-se o uso de três aulas de 50 minutos. A primeira pode ser dedicada à introdução dos conceitos a matrizes e ao Produto de Hadamard. A segunda, ao sistema de codificação e a terceira a reprodução com outros desenhos. Uma quarta aula pode ser adicionada para uso do sistema em computadores, caso haja conhecimento prévio e material disponíveis para isso.
- Nível de dificuldade: a atividade é indicada preferencialmente para o Ensino Médio, especialmente para turmas com conhecimentos prévios de matrizes. A complexidade é considerada intermediária a alta.
- Estratégia de ensino: comece retomando brevemente os conceitos de matriz, introduzir Produto de Hadamard e quadrado latino. Em seguida, mostre a aplicação desses conceitos para representar e transformar imagens, conectando com códigos de cor e pixels. Após isso, proponha que os alunos construam manualmente suas letras.
- Organização da turma: recomenda-se trabalho individual ou em duplas, especialmente durante a fase de encriptação e decodificação. Isso facilita a atenção ao processo e minimiza distrações ou perda de etapas lógicas.
- Ampliação da atividade: os alunos podem usar editores de planilhas eletrônicas para automatizar o processo de multiplicação ou ainda desenvolver códigos simples em linguagens como Python para aplicar o algoritmo de criptografia. Isso amplia o entendimento da codificação para contextos computacionais.

- Encerramento e sistematização: promova um momento de socialização das letras e os motivos de sua escolha. Estimule os alunos a explicar a lógica aplicada e os desafios enfrentados. Essa sistematização é essencial para consolidar os conceitos e valorizar o aspecto visual da matemática.

Atividade: Cada estudante construirá uma matriz 3×3 usando apenas os números 1 e 2, com o objetivo de desenhar uma letra. Por exemplo:

$$\text{Letra T} \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 2 & 1 & 2 \end{bmatrix} \qquad \text{Letra L} \begin{bmatrix} 1 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix} \qquad \text{Letra I} \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\text{Letra O} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad \text{Letra E} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix} \qquad \text{Letra C} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix}$$

Com isso, conforme exemplificado a seguir, o aluno criará sua própria matriz chave (K) e codificará com o auxílio de um quadrado latino (L), que deverá ser o mesmo para todos. Após a codificação, ele escolherá um colega e trocarão a matriz codificada juntamente com a chave, para que um decodifique a mensagem do outro. Ao final, caso desejem, cada um poderá falar sobre o dono da letra e o porquê de essa ser uma pessoa especial.

Objetivo: Compreender e conseguir executar o algoritmo de encriptação, tendo como elemento motivador a curiosidade pela mensagem do colega. Durante o processo, espera-se que o aluno se familiarize com os conceitos envolvidos no processo de encriptação com o Produto de Hadamard.

Exemplo:

Seja a matriz mensagem M:

$$M = \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 2 & 1 & 2 \end{bmatrix}$$

e a matriz chave K:

$$K = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

O quadrado latino L será de ordem 3 com elementos em $\{1, 2, 3\}$:

$$L = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

O criptograma C é obtido pelo produto de Hadamard sobre L:

$$\begin{aligned} C = M \odot_L K &= \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix} \\ &= \begin{bmatrix} L[m_{11}, k_{11}] & L[m_{12}, k_{12}] & L[m_{13}, k_{13}] \\ L[m_{21}, k_{21}] & L[m_{22}, k_{22}] & L[m_{23}, k_{23}] \\ L[m_{31}, k_{31}] & L[m_{32}, k_{32}] & L[m_{33}, k_{33}] \end{bmatrix} \\ &= \begin{bmatrix} L[1,2] & L[1,3] & L[1,1] \\ L[2,1] & L[1,2] & L[2,3] \\ L[2,3] & L[1,1] & L[2,2] \end{bmatrix} \\ &= \begin{bmatrix} 2 & 3 & 1 \\ 2 & 2 & 1 \\ 1 & 1 & 3 \end{bmatrix} \end{aligned}$$

Para recuperar a matriz mensagem M, precisamos de acesso a C, K e L. Para facilitar a visualização e o processo de descriptografia, tomemos a equação da matriz C mostrada anteriormente com destaque nos elementos de M que precisamos descobrir:

$$C = M \odot_L K = \begin{bmatrix} L[m_{11}, 2] & L[m_{12}, 3] & L[m_{13}, 1] \\ L[m_{21}, 1] & L[m_{22}, 2] & L[m_{23}, 3] \\ L[m_{31}, 3] & L[m_{32}, 1] & L[m_{33}, 2] \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 2 & 2 & 1 \\ 1 & 1 & 3 \end{bmatrix}$$

Os valores k_{ij} já estão distribuídos na matriz C pois a chave K precisa ser fornecida para quem irá descriptografar.

O processo de descriptação é simples e consiste na seguinte observação:

- m_{11} - Temos $c_{11} = L[m_{11}, 2] = 2$, então, ao olhar o quadrado latino L na coluna 2 podemos perceber que o resultado será 2 apenas na linha 1, o que garante ser $m_{11} = 1$.

- m_{12} - Temos $c_{12} = L[m_{12}, 3] = 3$, então, ao olhar o quadrado latino L na coluna 3 podemos perceber que o resultado será 3 apenas na linha 1, o que garante ser $m_{12} = 1$.

- m_{13} - Temos $c_{13} = L[m_{13}, 1] = 1$, então, ao olhar o quadrado latino L na coluna 1 podemos perceber que o resultado será 1 apenas na linha 1, o que garante ser $m_{13} = 1$.

- m_{21} - Temos $c_{21} = L[m_{21}, 1] = 2$, então, ao olhar o quadrado latino L na coluna 1 podemos perceber que o resultado será 2 apenas na linha 2, o que garante ser $m_{21} = 2$.

- m_{22} - Temos $c_{22} = L[m_{22}, 2] = 2$, então, ao olhar o quadrado latino L na coluna 2 podemos perceber que o resultado será 2 apenas na linha 1, o que garante ser $m_{22} = 1$.

- m_{23} - Temos $c_{23} = L[m_{23}, 3] = 1$, então, ao olhar o quadrado latino L na coluna 3 podemos perceber que o resultado será 1 apenas na linha 2, o que garante ser $m_{23} = 2$.

- m_{31} - Temos $c_{31} = L[m_{31}, 3] = 1$, então, ao olhar o quadrado latino L na coluna 3 podemos perceber que o resultado será 1 apenas na linha 2, o que garante ser $m_{31} = 2$.

- m_{32} - Temos $c_{32} = L[m_{32}, 1] = 1$, então, ao olhar o quadrado latino L na coluna 1 podemos perceber que o resultado será 1 apenas na linha 1, o que garante ser $m_{32} = 1$.

- m_{33} - Temos $c_{33} = L[m_{33}, 2] = 3$, então, ao olhar o quadrado latino L na coluna 2 podemos perceber que o resultado será 3 apenas na linha 2, o que garante ser $m_{33} = 2$.

Reflexão

- O Quadrado Latino não compromete a segurança do sistema por se tratar de uma matriz cuja função é garantir que a desencriptação seja possível. Sua propriedade de possuir um representante único no cruzamento de linha com coluna garante um único resultado possível no processo de desencriptação, qualquer que seja o Quadrado Latino.

- Usar mais entradas na matriz mensagem M exige um quadrado latino de dimensão maior, já que os valores de M são linhas em L, de modo que se tivesse a entrada 5 em M, por exemplo, L deveria ter uma quinta linha.

- Assim como em M, a matriz K deve ter suas entradas limitadas a dimensão do quadrado latino L.

Avaliação:

- Correção na construção das matrizes: Avalia-se se o aluno construiu corretamente a matriz mensagem (M), respeitando os valores permitidos pelo quadrado latino, e se elaborou uma matriz chave (K) compatível com as dimensões e restrições do sistema.

- Execução adequada do processo algorítmico: Observa-se se o aluno conseguiu aplicar corretamente o algoritmo de codificação $M \odot_L K$ e, na etapa de decodificação, identificar os elementos da matriz mensagem a partir da análise do quadrado latino e da matriz chave.

5.4.5 Atividade 5 – Matriz quebrada: reconstruindo o código perdido

Ilustração:

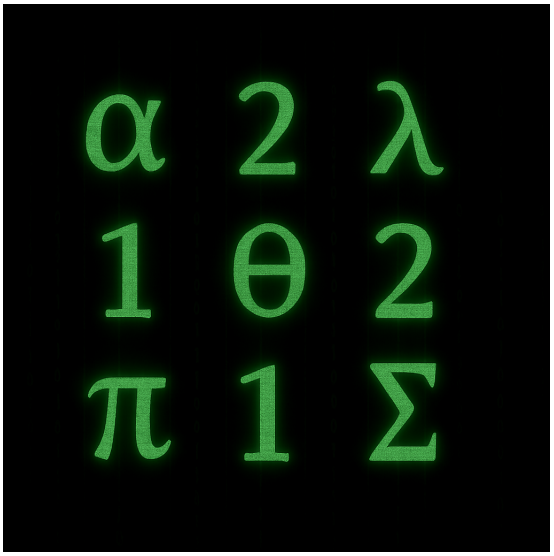


Figura 16 – Matriz quebrada

Fonte: Imagem gerada com o auxílio da inteligência artificial ChatGPT, OpenAI, em [07/2025].

Habilidades contempladas:

- (EF07MA05) Resolver um mesmo problema utilizando diferentes algoritmos.
- (EM13MAT203) Aplicar conceitos matemáticos no planejamento, na execução e na análise de ações envolvendo a utilização de aplicativos e a criação de planilhas

(para o controle de orçamento familiar, simuladores de cálculos de juros simples e compostos, entre outros), para tomar decisões.

- (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.
- (EM13MAT405) Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática

Orientações metodológicas:

- Tempo estimado: a atividade pode ser feita numa única aula de 50 minutos, mas faz-se necessário a compreensão plena da atividade 4.
- Nível de dificuldade: a atividade é indicada preferencialmente para o Ensino Médio.
- Estratégia de ensino: revise o funcionamento do sistema de encriptação apresentado na atividade 4 e as propriedades do quadrado latino, são esses elementos que possibilitam a solução do problema.
- Organização da turma: recomenda-se trabalho individual ou em duplas.

Enunciado:

Um computador teve a memória corrompida, e parte de uma encriptação armazenada nele foi perdida. Como o quadrado latino L é usado como base para outras encriptações, sua missão será tentar reconstruí-lo a partir dos dados remanescentes. Para certificar-se de que a reconstrução foi bem-sucedida, restaure também a mensagem encriptada C, de modo que seja possível verificar o funcionamento completo do sistema.

Considere as seguintes matrizes de ordem 3×3:

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix}, \quad K = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 2 \\ 3 & 2 & 3 \end{bmatrix}$$

Seja o quadrado latino L dado por:

$$L = \begin{bmatrix} 2 & 3 & 1 \\ \_\_ & \_\_ & \_\_ \\ \_\_ & \_\_ & \_\_ \end{bmatrix}$$

O produto de Hadamard parametrizado pelo quadrado latino L é definido como:

$$C = M \odot_L K \quad \text{tal que} \quad c_{ij} = L[m_{ij}, k_{ij}]$$

Aplicando essa operação:

$$C = \begin{bmatrix} L[1,1] & L[1,2] & L[1,3] \\ L[2,1] & L[1,2] & L[2,2] \\ L[1,3] & L[1,2] & L[1,3] \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 3 & \_\_ \\ \_\_ & \_\_ & \_\_ \end{bmatrix}$$

Resposta:

$$L = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{bmatrix}, \quad C = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 3 & 1 \\ 1 & 3 & 1 \end{bmatrix}$$

5.4.6 Atividade 6 – Produto de Hadamard: Criptografando imagens

Habilidades contempladas:

- (EF07MA05) Resolver um mesmo problema utilizando diferentes algoritmos.
- (EM13MAT203) Aplicar conceitos matemáticos no planejamento, na execução e na análise de ações envolvendo a utilização de aplicativos e a criação de planilhas (para o controle de orçamento familiar, simuladores de cálculos de juros simples e compostos, entre outros), para tomar decisões.
- (EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.
- (EM13MAT405) Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática

Orientações metodológicas:

- Tempo estimado: recomenda-se a aplicação da atividade anterior como pré-requisito. A inclusão das imagens é simples, dado que a atividade anterior foi perfeitamente entendida. O tempo estimado é de uma aula de 50 minutos para introdução e aplicação do conceito de imagens ao processo de encriptação já estudado.
- Nível de dificuldade: a atividade é indicada preferencialmente para o Ensino Médio, especialmente para turmas com conhecimentos prévios de matrizes. A complexidade é considerada intermediária a alta.

- Organização da turma: recomenda-se trabalho individual ou em duplas, especialmente durante a fase de encriptação e decodificação. Isso facilita a atenção ao processo e minimiza distrações ou perda de etapas lógicas.

- Potencial interdisciplinar: a atividade permite articulações com Artes (representação visual, construção de imagens por cor e forma), Informática (processamento digital de imagens, algoritmos de criptografia) e Física (conceito de pixel, resolução e codificação de sinais).

- Ampliação da atividade: os alunos podem usar editores de planilhas eletrônicas para automatizar o processo de multiplicação ou ainda desenvolver códigos simples em linguagens como Python para aplicar o algoritmo de criptografia. Isso amplia o entendimento da codificação para contextos computacionais.

- Encerramento e sistematização: promova um momento de socialização das imagens e dos processos utilizados. Estimule os alunos a explicar a lógica aplicada e os desafios enfrentados. Essa sistematização é essencial para consolidar os conceitos e valorizar o aspecto visual da matemática.

Nesta atividade, mostraremos como é possível utilizar o Produto de Hadamard para criptografar imagens. O método consiste em associar números a pixels e, por meio de matrizes, gerar uma imagem. No início do Capítulo 3, por meio da Figura 10, ilustramos como era possível representar um animalzinho com matrizes. Cada elemento da matriz representa um pixel; assim, quanto mais detalhada for a imagem, maior deverá ser a matriz e maior será o poder de processamento necessário.[1]

A fim de facilitar a compreensão do sistema, optamos por aplicar os mesmos valores da atividade anterior, trazendo ao leitor números e operações já familiares, permitindo que ele se concentre na aplicação gráfica.

Dada a seguinte associação:

Número	**Cor**
1	
2	
3	

construa uma matriz 3×3 usando apenas os números 1 e 2, com o objetivo de desenhar uma letra.

[1] Uma aplicação analógica dessa ideia pode ser observada na arte de retratar personalidades com Cubos de Rubik, que contêm seis cores e são compostos por dezenas de pequenos cubos.

Após isso, crie uma matriz chave (K) com números aleatórios e execute o processo de encriptação com um quadrado latino (L) qualquer. Afim de não se criar a necessidade de encontrar um quadrado latino mais complexo, limitaremos as entradas da matriz K aos naturais menores que ou iguais a 3, de modo que a matriz L tenha dimensão 3×3. Possível solução de um aluno:

$$M = \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 2 \\ 2 & 1 & 2 \end{bmatrix} = \begin{bmatrix} \blacksquare & \blacksquare & \blacksquare \\ \square & \blacksquare & \square \\ \square & \blacksquare & \square \end{bmatrix},$$

$$K = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} \square & \blacksquare & \blacksquare \\ \blacksquare & \square & \blacksquare \\ \blacksquare & \blacksquare & \square \end{bmatrix}$$

$$L = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} = \begin{bmatrix} \blacksquare & \square & \blacksquare \\ \square & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \square \end{bmatrix}$$

O criptograma C é obtido pelo produto de Hadamard sobre L:

$$C = M \odot_L K = \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix} = \begin{bmatrix} L[m_{11}, k_{11}] & L[m_{12}, k_{12}] & L[m_{13}, k_{13}] \\ L[m_{21}, k_{21}] & L[m_{22}, k_{22}] & L[m_{23}, k_{23}] \\ L[m_{31}, k_{31}] & L[m_{32}, k_{32}] & L[m_{33}, k_{33}] \end{bmatrix}$$

$$= \begin{bmatrix} L[1,2] & L[1,3] & L[1,1] \\ L[2,1] & L[1,2] & L[2,3] \\ L[2,3] & L[1,1] & L[2,2] \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 2 & 2 & 1 \\ 1 & 1 & 3 \end{bmatrix} = \begin{bmatrix} \square & \blacksquare & \blacksquare \\ \square & \square & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare \end{bmatrix}$$

Para recuperar a matriz mensagem M, precisamos de acesso a C, K e L. Para facilitar a visualização e o processo de descriptografia, tomemos a equação da matriz C mostrada anteriormente com destaque nos elementos de M que precisamos descobrir:

$$C = M \odot_L K = \begin{bmatrix} L[m_{11}, 2] & L[m_{12}, 3] & L[m_{13}, 1] \\ L[m_{21}, 1] & L[m_{22}, 2] & L[m_{23}, 3] \\ L[m_{31}, 3] & L[m_{32}, 1] & L[m_{33}, 2] \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 \\ 2 & 2 & 1 \\ 1 & 1 & 3 \end{bmatrix} = \begin{bmatrix} \square & \blacksquare & \blacksquare \\ \square & \square & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare \end{bmatrix}$$

Os valores k_{ij} já estão distribuídos na matriz C pois a chave K precisa ser fornecida para quem irá descriptografar.

O processo de descriptação é simples e consiste na seguinte observação:

- m_{11} - Temos $c_{11} = L[m_{11}, 2] = 2$, então, ao olhar o quadrado latino L na coluna 2 podemos perceber que o resultado será 2 apenas na linha 1, o que garante ser $m_{11} = 1 = \blacksquare$

- m_{12} - Temos $c_{12} = L[m_{12}, 3] = 3$, então, ao olhar o quadrado latino L na coluna 3 podemos perceber que o resultado será 3 apenas na linha 1, o que garante ser $m_{12} = 1 =$ ■

- m_{13} - Temos $c_{13} = L[m_{13}, 1] = 1$, então, ao olhar o quadrado latino L na coluna 1 podemos perceber que o resultado será 1 apenas na linha 1, o que garante ser $m_{13} = 1 =$ ■.

- m_{21} - Temos $c_{21} = L[m_{21}, 1] = 2$, então, ao olhar o quadrado latino L na coluna 1 podemos perceber que o resultado será 2 apenas na linha 2, o que garante ser $m_{21} = 2 =$ □.

- m_{22} - Temos $c_{22} = L[m_{22}, 2] = 2$, então, ao olhar o quadrado latino L na coluna 2 podemos perceber que o resultado será 2 apenas na linha 1, o que garante ser $m_{22} = 1 =$ ■.

- m_{23} - Temos $c_{23} = L[m_{23}, 3] = 1$, então, ao olhar o quadrado latino L na coluna 3 podemos perceber que o resultado será 1 apenas na linha 2, o que garante ser $m_{23} = 2 =$ □.

- m_{31} - Temos $c_{31} = L[m_{31}, 3] = 1$, então, ao olhar o quadrado latino L na coluna 3 podemos perceber que o resultado será 1 apenas na linha 2, o que garante ser $m_{31} = 2 =$ □.

- m_{32} - Temos $c_{32} = L[m_{32}, 1] = 1$, então, ao olhar o quadrado latino L na coluna 1 podemos perceber que o resultado será 1 apenas na linha 1, o que garante ser $m_{32} = 1 =$ ■.

- m_{33} - Temos $c_{33} = L[m_{33}, 2] = 3$, então, ao olhar o quadrado latino L na coluna 2 podemos perceber que o resultado será 3 apenas na linha 2, o que garante ser $m_{33} = 2 =$ □

Avaliação:

- Correção na construção das matrizes: Avalia-se se o aluno construiu corretamente a matriz mensagem (M), respeitando os valores permitidos pelo quadrado latino, e se elaborou uma matriz chave (K) compatível com as dimensões e restrições do sistema.

- Execução adequada do processo algorítmico: Observa-se se o aluno conseguiu aplicar corretamente o algoritmo de codificação $M \odot_L K$ e, na etapa de decodificação, identificar os elementos da matriz mensagem a partir da análise do quadrado latino e da matriz chave.

6 Considerações Finais

Este trabalho teve por objetivo principal explorar o Produto de Hadamard, objeto que, conforme constatado em nossas pesquisas, não possui registros de investigações na área da Matemática em nosso país, especialmente no que diz respeito ao ensino básico. Verificamos tratar-se de um conceito presente no imaginário intuitivo dos alunos, quando estudam o produto usual de matrizes, além da possibilidade de associar esse produto a sistemas de criptografia matricial.

Além de apresentar as propriedades essenciais do Produto de Hadamard, foram discutidas suas relações com outros conceitos importantes da Álgebra Linear, como o produto usual de matrizes. Essa abordagem permitiu não apenas aprofundar a compreensão teórica, mas também oferecer subsídios para possíveis aplicações em áreas diversas, como a criptografia.

Nesse contexto, o trabalho propôs uma análise ampla no tempo e detalhada nos conceitos, com uma incursão histórica que resgatou desde os primórdios das técnicas de encriptação até métodos mais recentes. Foram apresentados e discutidos sistemas clássicos, como a *cítale espartano*, a *cifra de César* e o *trilho de trem*, destacando-se suas lógicas internas, seus pontos fortes e suas vulnerabilidades. Além disso, examinou-se o papel da criptografia ao longo da história, enfatizando sua importância como ferramenta de proteção e transmissão segura de informações.

O ápice do trabalho reside na proposta de um sistema criptográfico fundamentado no Produto de Hadamard, que, mediante o uso de quadrados latinos, permite a construção de um esquema de encriptação inovador. Utilizado em computadores para ocultação de caracteres, esse sistema se baseia na ideia de um produto matricial modificado, utilizando a estrutura do Produto de Hadamard em combinação com os quadrados latinos. Nas camadas mais baixas de proteção, fazendo uso de uma construção analógica é possível formular dinâmicas com elementos de interesse comunicativo que exercitam as propriedades desse produto além de sistemas de encriptação e algorítimo.

Além da fundamentação teórica, dedicou-se uma parte significativa desta dissertação ao desenvolvimento de propostas didáticas que visam à aplicação prática dos conhecimentos adquiridos. Foram elaboradas atividades direcionadas ao ensino básico, que permitem aos estudantes vivenciar experiências com sistemas criptográficos de forma lúdica e contextualizada. As atividades propostas, que incluem a utilização da *cítale espartano*, da *cifra de César*, do *trilho de trem* e do próprio Produto de Hadamard, têm por objetivo fomentar a curiosidade, a criatividade e o pensamento lógico, aspectos fundamentais para o desenvolvimento das competências matemáticas.

Incluir essas atividades reforça a convicção de que a Matemática não nem sempre,

mas por vezes, pode ser ensinada de maneira significativa, aproximando-se do cotidiano dos estudantes e valorizando a resolução de problemas em contextos reais ou simulados. Nesse sentido, a utilização da criptografia como tema gerador revela-se uma estratégia eficaz para motivar o aprendizado, além de proporcionar um ambiente propício ao desenvolvimento de habilidades interdisciplinares.

Por fim, acredita-se que este trabalho tenha alcançado seus objetivos, tanto no que diz respeito à sistematização, divulgação e aprofundamento do conhecimento sobre o Produto de Hadamard, como também na explanação de sistemas de criptografia, incluindo aquele que envolve esse notável produto. Espera-se que as reflexões, os exemplos e as atividades aqui apresentados possam servir de inspiração para professores, pesquisadores e estudantes interessados em ampliar suas abordagens didáticas, bem como para aqueles que desejam explorar novas possibilidades no campo da criptografia e da Matemática aplicada.

Como perspectiva para trabalhos futuros, sugere-se a ampliação das investigações sobre a eficácia didática das atividades propostas, mediante sua aplicação em ambientes escolares, bem como o aprofundamento em aspectos mais avançados da criptografia Matemática, que possam integrar outras estruturas algébricas e combinatórias associadas ao Produto de Hadamard.

Referências

BARAHMAND, A. On the definition of matrix multiplication. *International Journal of Mathematical Education in Science and Technology*, v. 51, n. 7, p. 1137–1145, 2020. Citado na página 37.

Base Nacional Comum Curricular. *Base Nacional Comum Curricular*. Brasília: Ministério da Educação, 2018. Disponível em: <https://basenacionalcomum.mec.gov.br/>. Citado 3 vezes nas páginas 21, 82 e 90.

BASSANEZI, R. R. *Modelagem Matemática: uma nova forma de ver o mundo*. São Paulo: Editora Contexto, 2002. Citado na página 84.

BONFIM, D. H. *Criptografia RSA*. Tese (Doutorado) — Universidade de São Paulo, 2017. Citado na página 39.

CAMPOS, M. A.; FARIAS, L. M. S. A educação matemática e o ensino de álgebra na perspectiva de desenvolvimento do pensamento algébrico. *Revista Binacional Brasil-Argentina: Diálogo entre as ciências*, v. 9, n. 1, p. 167–188, 2020. Citado na página 81.

CARO-LOPERA, F. J.; LEIVA, V.; BALAKRISHNAN, N. Connection between the hadamard and matrix products with an application to matrix-variate birnbaum–saunders distributions. *Journal of Multivariate Analysis*, Elsevier, v. 104, n. 1, p. 126–139, 2012. Citado 2 vezes nas páginas 56 e 62.

CASSIANO, G.; GÓES, C. B.; NEVES, B. C. As tecnologias digitais no contexto educacional para a autonomia dos sujeitos. *Revista Fontes Documentais, Aracaju*, v. 2, n. 3, p. 43–58, 2019. Citado 2 vezes nas páginas 21 e 22.

CRESWELL, J. W. Projeto de pesquisa: métodos qualitativo, quantitativo e misto. Artmed, 2010. Citado na página 32.

DONIAK, M. H. *Estudo da transformada de walsh-hadamard aplicada à transmissão ofdm*. Tese (Doutorado em Engenharia Elétrica) — Universidade Federal de Santa Catarina, Centro Tecnológico, Florianópolis, 2006. Citado 2 vezes nas páginas 22 e 36.

DéNES, J.; KEEDWELL, A. D. *Latin Squares and Their Applications*. New York: Academic Press, 1991. ISBN 9780122091309. Citado 2 vezes nas páginas 74 e 75.

ERIC – Education Resources Information Center. *ERIC – Education Resources Information Center*. 2025. <https://eric.ed.gov>. Acesso em: 12 jul. 2025. Citado na página 39.

FALCÓN, R. M. et al. A computational approach to analyze the hadamard quasigroup product. *Electronic Research Archive*, v. 31, n. 6, p. 3245–3263, 2023. Disponível em: <https://www.aimspress.com/article/id/64262c54ba35de6af0322840>. Citado 5 vezes nas páginas 23, 33, 73, 76 e 84.

Folha de S. P. *USP lidera ranking geral pelo quarto ano seguido e ocupa o primeiro posto em 33 carreiras avaliadas*. 2024. Acesso em 10 de setembro de 2025. Disponível em: <https://ruf.folha.uol.com.br/2024/noticias/usp-lidera-ranking-geral-pelo-quarto-ano-seguido-e-ocupa-o-primeiro-posto-em-33-carreiras-avaliadas.shtml>. Citado na página 35.

FREIRE, P. *Pedagogia do oprimido*. 17. ed. Rio de Janeiro: Paz e Terra, 1987. Citado na página 83.

FREUDENTHAL, H. *Revisiting Mathematics Education*. Dordrecht, Países Baixos: Springer, 1994. v. 9. 1–202 p. (Mathematics Education Library, 1). Citado na página 82.

G1 Piauí. *Decisão de juiz do Piauí manda tirar WhatsApp do ar em todo o Brasil*. 2015. Acesso em: 28 mar. 2025. Disponível em: <https://g1.globo.com/pi/piaui/noticia/2015/02/decisao-de-juiz-do-piaui-manda-tirar-whatsapp-do-ar-em-todo-o-brasil.html>. Citado na página 66.

G1 Tecnologia. *Justiça dos EUA manda Apple burlar criptografia do iPhone e ajudar o FBI*. 2016. Acesso em: 28 mar. 2025. Disponível em: <https://g1.globo.com/tecnologia/noticia/2016/02/justica-dos-eua-manda-apple-burlar-criptografia-do-iphone-e-ajudar-o-fbi.html>. Citado na página 66.

GALDINO, U. A. Monografia (Graduação em Matemática), *Teoria dos números e Criptografia com Aplicações Básicas*. Juazeiro do Norte: [s.n.], 2014. Disponível em: <<linksehouver>>. Acesso em: 8 set. 2025. Citado na página 39.

GLISTER, P. *Digital Literacy*. New York: John Wiley & Sons, 1997. Citado na página 21.

Google Acadêmico. *Google Acadêmico*. 2025. <https://scholar.google.com>. Acesso em: 12 jul. 2025. Citado na página 38.

HARARI, Y. N. *Sapiens: Uma Breve História da Humanidade*. São Paulo: Companhia das Letras, 2015. Tradução de Livia de Almeida e Janaína Marcoantonio. Citado 2 vezes nas páginas 79 e 80.

HE, X. et al. Neural collaborative filtering. In: *Proceedings of the 26th International Conference on World Wide Web*. [S.l.: s.n.], 2017. p. 173–182. Citado na página 50.

HORN, R. A.; JOHNSON, C. R. *Matrix analysis*. [S.l.]: Cambridge university press, 2012. Citado 2 vezes nas páginas 43 e 56.

InfoMoney. *Há cinco 'Petrobras' em bitcoins perdidos – e vale até hipnose para tentar recuperar*. 2024. Acesso em: 28 mar. 2025. Disponível em: <https://www.infomoney.com.br/onde-investir/ha-cinco-petrobras-em-bitcoins-perdidos-e-vale-ate-hipnose-para-tentar-recuperar/>. Citado na página 66.

Instituto Brasileiro de Geografia e Estatística (IBGE). *Em 2023, 87,2% das pessoas com 10 anos ou mais utilizaram internet*. 2024. <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet>. Publicado em 19 mar. 2024. Acesso em: 1 jul. 2025. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet>. Citado na página 21.

KISHKA, Z. et al. On hadamard and kronecker products over matrix of matrices. *General Letters in Mathematics*, v. 4, n. 1, p. 13–22, 2018. Citado na página 43.

MACEDO, N. D. de. *Iniciação à pesquisa bibliográfica*. [S.l.]: Edições Loyola, 1995. Citado na página 27.

MANN, R. *Brazil's Tax Burden: Highest in Latin America, Lowest in Returns*. The Rio Times, 2024. Acesso em 13 de julho de 2025. Disponível em: <https://www.riotimesonline.com/brazils-tax-burden-highest-in-latin-america-lowest-in-returns/>. Citado na página 53.

MARQUES, T. V. *Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula*. Dissertação (Dissertação (Mestrado Profissional em Matemática em Rede Nacional)) — Universidade Federal de Juiz de Fora, Juiz de Fora, 2013. Citado na página 40.

MESSIAS, M.; SÁ, P. F.; FONSECA, R. V. Um estudo diagnóstico sobre as dificuldades em matrizes. *Encontro Nacional de Educação de Matemática (ENEM), IX*, 2007. Citado 5 vezes nas páginas 15, 28, 29, 30 e 31.

MILLION, E. *The Hadamard Product*. 2007. Course notes / projeto acadêmico, University of Puget Sound (UPS). Disponível em: <http://buzzard.ups.edu/courses/2007spring/projects/million-paper.pdf>. Acesso em: 8 set. 2025. Citado na página 43.

Ministério da Educação (Brasil). *Anexo ao Parecer CNE/CEB n° 2/2022: Normas sobre Computação na Educação Básica – Complemento à Base Nacional Comum Curricular*. 2022. <http://portal.mec.gov.br/docman/fevereiro-2022-pdf/236791-anexo-ao-parecer-cneceb-n-2-2022-bncc-computacao/file>. Acesso em: 16 maio 2025. Citado na página 83.

MORAIS, G. D. *A Matemática Via Algoritmo de Criptografia El Gamal*. Dissertação (Dissertação (Mestrado Profissional em Matemática em Rede Nacional)) — Universidade Federal da Paraíba, João Pessoa, 2013. Citado na página 40.

MORGADO, A. C. d. O. et al. *Coleção do Professor de Matemática*. [S.l.]: Sociedade Brasileira de Matemática, 1991. ISBN 8585818018. Citado na página 68.

NEUDECKER, H. On the matrix formulation of kaiser's varimax criterion. *Psychometrika*, v. 46, n. 3, p. 343–345, 1981. Citado na página 38.

PAIXÃO, J. S. d. *Criptografia: história, atividades e divulgação científica*. Tese (Doutorado) — Universidade de São Paulo, 2020. Citado 2 vezes nas páginas 39 e 40.

PESSOA, S.; FILHO, F. de H. B. Acesso ao ensino superior no brasil. In: CAMARGO, R. B. de; BELLUZZO, L. G. (Ed.). *O ensino superior no Brasil: reflexões e perspectivas*. Editora UFRJ, 2007. Acessado em: 21 fev. 2025. Disponível em: <https://books.scielo.org/id/n656x/pdf/sampaio-9788523212117-03.pdf>. Citado na página 28.

RODRIGUES, M. A. *Tópicos de criptografia para ensino médio*. Tese (Doutorado) — Universidade de São Paulo, 2016. Citado na página 39.

Secretaria da Educação do Estado da Paraíba. *Proposta Curricular do Ensino Médio da Paraíba*. 2023. Acesso em: 09 maio 2025. Disponível em: <https://paraiba.pb.gov.br/arquivos/pdfs/PropostaCurriculardoEnsinoMdiodaParabaPCEMPB23.pdf>. Citado na página 81.

Secretaria de Estado da Educação da Paraíba. *Proposta Curricular do Ensino Médio da Paraíba (PCEM-PB)*. 2023. Acesso em: 14 fev. 2025. Disponível em: <https://paraiba.pb.gov.br/arquivos/pdfs/PropostaCurriculardoEnsinoMdiodaParabaPCEMPB23.pdf>. Citado 2 vezes nas páginas 21 e 84.

SILVA, J. dos S. *Alguns métodos de criptografia*. Dissertação (Dissertação de Mestrado) — Universidade Estadual da Paraíba, Campina Grande, PB, 2016. Acesso Aberto. Disponível em: <https://tede.bc.uepb.edu.br/jspui/handle/tede/2619>. Citado na página 39.

SINGH, S. *O livro dos códigos*. [S.l.]: Editora Record, 2001. Citado 8 vezes nas páginas 40, 65, 67, 70, 71, 72, 73 e 84.

Sociedade Brasileira de Matemática. *Catálogo de disciplinas – PROFMAT*. 2017. <https://sbm.org.br/profmat/wp-content/uploads/sites/4/sites/4/2021/10/Catalogo-de-Disciplinas_2017.pdf>. Acesso em: 3 jul. 2025. Citado na página 33.

Sociedade Brasileira de Matemática (SBM). *Dissertações do PROFMAT - Mestrado Profissional em Matemática em Rede Nacional*. 2024. Acesso em: 13 nov. 2024. Disponível em: <https://profmat-sbm.org.br/dissertacoes/>. Citado 2 vezes nas páginas 35 e 36.

SOUSA, A. S. D.; OLIVEIRA, G. S. D.; ALVES, L. H. A pesquisa bibliográfica: princípios e fundamentos. *Cadernos da FUCAMP*, v. 20, n. 43, 2021. Citado na página 27.

Superinteressante. *A arte da traição*. 2020. Acesso em: 04 abr. 2025. Disponível em: <https://super.abril.com.br/historia/a-arte-da-traicao/>. Citado na página 68.

THEODORSON, G. *Modern dictionary of sociology*. [S.l.]: Thomas Y. Crowell, 1969. Citado na página 24.

WhatsApp. *Perguntas Frequentes do WhatsApp*. 2025. Acesso em: 28 mar. 2025. Disponível em: <https://faq.whatsapp.com/820124435853543/?locale=pt_BR>. Citado na página 66.