Revista ARACÊ
ISSN: 2358-2472

UM SISTEMA CRIPTOGRÁFICO PEDAGÓGICO BASEADO NO PRODUTO DE HADAMARD: POTENCIALIDADES PARA O ENSINO MÉDIO

A CRYPTOGRAPHIC EDUCATIONAL SYSTEM BASED ON THE HADAMARD PRODUCT: POTENTIAL FOR HIGH SCHOOL EDUCATION

UN SISTEMA EDUCATIVO CRIPTOGRÁFICO BASADO EN EL PRODUCTO HADAMARD: POTENCIAL PARA LA EDUCACIÓN SECUNDARIA

https://doi.org/10.56238/arev7n12-199

Data de submissão: 18/11/2025 **Data de publicação:** 18/12/2025

Joaquim Denilson de Souza Silva
M.Sc.
Instituição: EMEF Flaviano Ribeiro Coutinho
E-mail: denilsonjoaquim@gmail.com
Lattes: http://lattes.cnpq.br/7386627234177474

Luiz Antônio da Silva Medeiros
D.Sc.
Instituição: Universidade Federal de Campina Grande
E-mail: luiz.silva@professor.ufcg.edu.br
Lattes: http://lattes.cnpq.br/5778546806126449

José Lucas Galdino da Silva
D.Sc.
Instituição: Universidade Federal de Campina Grande
E-mail: jose.silva@professor.ufcg.edu.br
Lattes: http://lattes.cnpq.br/0968537800835808

RESUMO
Este trabalho utiliza o produto de Hadamard entre matrizes, propondo-o como recurso pedagógico para o ensino de conceitos matemáticos e criptográficos na Educação Básica. A partir de um levantamento bibliográfico nacional e internacional, constatou-se a ausência do Produto de Hadamard como objeto de estudo no currículo escolar e em trabalhos brasileiros voltados ao ensino de Matemática. A pesquisa internacional indica que, embora essa operação seja mencionada em contextos avançados, ainda não havia registros de sua aplicação no Ensino Básico. Nesse cenário, desenvolveu-se um sistema de embaralhamento com matrizes e elaborou-se uma adaptação desse sistema para a encriptação de imagens, utilizando elementos de complexidade suficientemente simples para implementação no Ensino Médio, 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.

Revista ARACÊ
ISSN: 2358-2472

ABSTRACT
This work utilizes the Hadamard product between matrices, proposing it as a pedagogical resource for teaching mathematical and cryptographic concepts in Basic Education. Based on a national and international bibliographic survey, the absence of the Hadamard product as an object of study in the school curriculum and in Brazilian works focused on mathematics education was noted. International research indicates that, although this operation is mentioned in advanced contexts, there were no records of its application in Basic Education. In this scenario, a matrix scrambling system was developed, and an adaptation of this system for image encryption was elaborated, using elements of sufficiently simple complexity for implementation in High School, focusing on its potential as a tool for motivation and contextualization of mathematics. The proposal is based on Realistic Mathematics Education, Mathematical Modeling, and the competencies foreseen by the BNCC (Brazilian National Curriculum Base), seeking to promote more meaningful learning and bring students closer to contemporary contexts in which cryptography is embedded.

Keywords: Hadamard Product. Cryptography. Teaching Mathematics.

RESUMEN
Este trabajo utiliza el producto Hadamard entre matrices, proponiéndolo como recurso pedagógico para la enseñanza de conceptos matemáticos y criptográficos en Educación Básica. Con base en una revisión bibliográfica nacional e internacional, se observó la ausencia del producto Hadamard como objeto de estudio en el currículo escolar y en trabajos brasileños enfocados en la educación matemática. Investigaciones internacionales indican que, si bien esta operación se menciona en contextos avanzados, no existen registros de su aplicación en Educación Básica. En este contexto, se desarrolló un sistema de codificación de matrices y se elaboró una adaptación de este sistema para el cifrado de imágenes, utilizando elementos de complejidad suficientemente simple para su implementación en la Educación Secundaria, centrándose en su potencial como herramienta de motivación y contextualización de las matemáticas. La propuesta se basa en la Educación Matemática Realista, el Modelado Matemático y las competencias previstas por la BNCC (Base Curricular Nacional de Brasil), buscando promover un aprendizaje más significativo y acercar a los estudiantes a los contextos contemporáneos donde la criptografía está presente.

Palabras clave: Producto Hadamard. Criptografía. Enseñanza de las Matemáticas.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

A criptografia, em sua forma mais simples, pode ser entendida como a arte de ocultar informações. Desde as primeiras civilizações, reconheceu-se a necessidade de transmitir mensagens com segurança, protegendo-as de leitores indesejados. Por essa razão, técnicas de codificação surgiram muito antes dos computadores e muito antes da matemática moderna. Entre os registros históricos mais conhecidos está a *scytale*: um cilindro onde uma fita era enrolada em espiral. A mensagem era escrita ao longo do cilindro, linha por linha, e, ao desenrolar a fita, tornava-se ilegível, podendo ser recuperada apenas quando novamente 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 (SINGH, 2013).

Figura 1 - Representação da *Scytale*

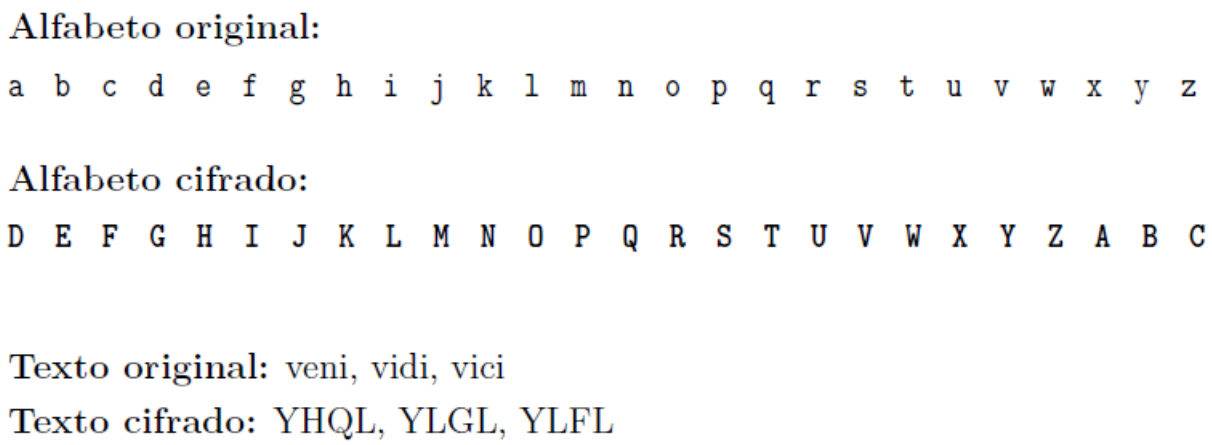
Fonte: Wikipédia, 2025.

No Império Romano, Júlio César popularizou outra técnica de ocultação: a substituição alfabética por deslocamento, hoje conhecida como *Cifra de César* (COUTINHO, 2016). Segundo Singh (2001), encontra-se na obra As vidas dos Césares, escrito no século II por Suetônio, um processo que consistia em substituir cada letra da mensagem pela terceira subsequente no alfabeto. Para facilitar o processo de escrita era produzido um alfabeto cifrado, guiando as substituições. Abaixo temos um exemplo da

tabela de encriptação e de uma mensagem encriptada.

Revista ARACÊ
ISSN: 2358-2472

Figura 2 - Alfabeto Cifrado



Fonte: Reproduzida do texto Singh (2001).

Suetônio faz referência apenas a chave 3, isto é, o deslocamento de três posições no alfabeto utilizado por César. Entretanto, é evidente que outras chaves poderiam ser aplicadas e, considerando um alfabeto de 26 letras, existem 26 possibilidades de encriptação usando o algoritmo da Cifra de César. Isso evidencia 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.

Apesar de terem sido criadas com propósitos bélicos, as duas técnicas citadas apresentam simplicidade suficiente para serem implementadas na educação básica como recursos pedagógicos, interdisciplinares e motivadores, como discutido em Rosseto (2018). Isso permite explorar a matemática de forma significativa e contextualizada, além de promover discussões sobre a necessidade do sigilo em muitas transações envolvendo as redes sociais, oportunizando a criação de ambientes reflexivos e colaborativos para entender e explicar a realidade de forma crítica, significativa e ética envolvendo as tecnologias digitais de comunicação e informação como sugerem algumas competências da Base Nacional Comum Curricular para o Ensino Médio (BRASIL, 2025). Destaca-se, nesse sentido, a habilidade “EF09CO05”, que orienta o estudante do 9ºano a “analisar técnicas de criptografia para armazenamento e transmissão de dados” (BRASIL, 2022, p. 54). Dessa forma, conteúdos abstratos passam a ter utilidade imediata, ganhando formas concretas de modo a favorecer o engajamento e interesse dos estudantes.

A Base Nacional Comum Curricular passou por um processo de ampliação ao incorporar oficialmente o Componente Curricular de Computação. Essa integração foi normatizada pela Resolução CNE/CEB nº 1/2022, que estabelece as ‘Normas sobre Computação na Educação Básica – Complemento à BNCC’ normativa que possibilita a construção do desenvolvimento do pensamento computacional, da cultura digital e da lógica. A partir dessa resolução, o ensino de Computação passa

Revista ARACÊ
ISSN: 2358-2472

a fazer parte da organização curricular das redes de ensino, legitimando o trabalho pedagógico com temas como criptografia, segurança da informação e algoritmos no contexto da Educação Básica.

Com o avanço das tecnologias digitais, a criptografia deixou de ser apenas um recurso militar e passou a integrar atividades cotidianas. Hoje, praticamente toda comunicação digital — transações bancárias, mensagens de celular, e-mails e até jogos online — depende de algoritmos avançados para garantir segurança, integridade e privacidade. Segundo o 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, em Brasil (2025), sua 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 relacionado aos meios de comunicação e informação digitais e possa propor melhorias ou até mesmo novos sistemas.

Pesquisas demonstram que o trabalho pedagógico com criptografia é viável e produtivo no contexto escolar permitindo atividades interdisciplinares que envolvem História da Matemática, Matemática, Computação e até Língua Portuguesa. Há registros de propostas didáticas baseadas em criptografia como ferramenta pedagógica, como em Batista e Fonseca (2025), Bruxelas (2017) e Silva (2019). Contudo, tais trabalhos frequentemente recorrem à criptografia RSA ou a algoritmos que existem conhecimentos avançados de Teoria de Números, o que restringe sua aplicabilidade em níveis introdutórios.

Nesse sentido, o produto de Hadamard destaca-se como possibilidade alternativa. Definido como a multiplicação elemento a elemento entre duas matrizes de mesma dimensão, possui propriedades singulares que o diferenciam da multiplicação matricial convencional, como a facilidade das operações e comutatividade do produto. Tais características favorecem aplicações criptográficas acessíveis, permitindo a criação de sistemas de transformação e embaralhamento de dados com exigência matemática reduzida. Apesar desse potencial, tal produto não é abordado em trabalhos nacionais (e até mesmo internacionais) relacionados ao ensino de Matemática, sendo mais comum em aplicações de engenharia ou em estudos avançados de pós-graduação.

Revista ARACÊ
ISSN: 2358-2472

Desta forma, este artigo trata-se de uma pesquisa exploratória, que se constitui como parte de uma dissertação do Mestrado Profissional em Matemática (SILVA, 2025), cujo levantamento bibliográfico foi iniciado em novembro de 2024. Buscas em bases nacionais, como o Banco de Dissertações da USP, SciELO e Google Acadêmico, não identificaram trabalhos que utilizassem o produto de Hadamard como objeto de estudo na Educação Matemática. Consultas adicionais via ferramentas de I.A. também não retornaram resultados relevantes. Os poucos trabalhos encontrados no Brasil pertenciam à área da engenharia, como a dissertação de mestrado em Engenharia Elétrica de Doniak (2006). Em bases internacionais, 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 resultados obtidos revelaram predominantemente materiais voltados a conteúdos avançados. Um caso atípico é Barahmand (2020), que discute justificativas conceituais para o produto usual de matrizes e menciona o produto de Hadamard apenas como exemplo secundário. Também foi utilizada a base de dados ERIC, especializada em educação, aplicando o termo “Hadamard product” apenas um resultado foi retornado, e aplicava-se ao ensino superior.

Diante dessa lacuna, o presente artigo tem como objetivo investigar o Produto de Hadamard e propor sua utilização em um sistema criptográfico simples, acessível a estudantes do Ensino Médio. Busca-se aproximar teoria e prática por meio de atividades que evidenciem a aplicabilidade do conceito em processos de encriptação digital e analógica, contribuindo para uma aprendizagem significativa e conectada à contemporaneidade. Além disso, pretende-se estimular reflexões sobre o papel das definições matemáticas e sobre como operações distintas podem emergir de necessidades específicas, ampliando a compreensão dos estudantes acerca da natureza da Matemática e de suas aplicações.

2 METODOLOGIA

O presente estudo caracteriza-se como uma pesquisa bibliográfica de natureza exploratória, com abordagem qualitativa, voltada à sistematização conceitual e à proposição de aplicações didáticas. Conforme Theodorson e Theodorson (1969), pesquisas exploratórias têm por finalidade promover a familiarização com o fenômeno investigado, permitindo uma compreensão inicial mais

Revista ARACÊ
ISSN: 2358-2472

precisa e orientando etapas posteriores do estudo. A investigação constatou a inexistência do tema na literatura educacional em Matemática, evidenciando uma lacuna significativa a ser preenchida. Dessa forma, nosso trabalho pôde, especialmente no âmbito nacional, divulgar o Produto de Hadamard como ponto de partida para pesquisas na graduação e na pós-graduação, mas, sobretudo e especialmente, apresentar uma conexão inédita entre esse produto e o ensino básico

Inicialmente, procedeu-se a uma revisão teórica sobre o Produto de Hadamard, contemplando suas definições formais, propriedades elementares e potenciais aplicações em diferentes áreas, com ênfase particular no campo da criptografia. Esse estudo buscou evidenciar as distinções entre o Produto de Hadamard e a multiplicação matricial convencional, destacando a relevância de sua estrutura algébrica para a construção de sistemas de codificação e transformação de dados.

Complementarmente, com base em Singh (2013), realizou-se uma análise comparativa entre os principais processos criptográficos históricos. Essa análise possibilitou discutir o potencial pedagógico desses métodos, tanto sob uma perspectiva conceitual quanto aplicada, o que forneceu subsídios para a elaboração de atividades didáticas de criptografia com nível de complexidade adequado para aplicação no ensino fundamental. Essas atividades foram sistematizadas, detalhadas e podem ser consultadas em nosso trabalho principal Silva (2025).

3 RESULTADOS

Nesta seção, apresentamos o desenvolvimento do sistema criptográfico proposto, estruturando-o a partir das propriedades do Produto de Hadamard e de sua integração com quadrados latinos. O objetivo é evidenciar como conceitos matriciais simples podem ser articulados para formar um sistema de encriptação acessível, explorável em sala de aula e matematicamente consistente.

Adotamos as seguintes notações:

- $M_{m\times n}(R)$: O conjunto de matrizes de ordem $m \times n$ com entradas reais.
- $M_n(R)$: O conjunto das matrizes quadradas de ordem n com entradas reais.
- $N = \{1, 2, 3, \cdots\}$

Definição: Dadas $A = [a_{ij}]\ e\ B = [b_{ij}] \in M_{m\times n}(R)$, definimos o Produto de Hadamard como

$$A \circ B = \left[a_{ij} \cdot b_{ij}\right] \in M_{m\times n}(R), \qquad (1)$$

onde a operação "·" denota o produto usual dos reais.

Revista ARACÊ
ISSN: 2358-2472

Dadas $A, B, C \in M_{m\times n}(R)$, $\alpha \in R$, com base nos trabalhos de Million (2007), Kishka et al. (2018) e por construção própria, podemos verificar facilmente as seguintes propriedades:

- *Comutatividade*: $A \circ B = B \circ A$;
- *Associatividade*: $A \circ (B \circ C) = (A \circ B) \circ C$;
- *Distributividade em relação a adição*: $C \circ (A + B) = (C \circ A) + (C \circ B)$;
- *Distributividade e associatividade em relação ao produto por escalar*: $\alpha \cdot (A \circ B) = (\alpha \cdot A) \circ B = A \circ (\alpha \cdot B)$;
- *Transposta*: $(A \circ B)^T = A^T \circ B^T$;
- *Existência de elemento neutro:* A matriz $J_{m\times n}$ definida por

$$J_{m\times n} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix} \qquad (2)$$

é denominada Matriz Unidade ou Matriz de Uns. Para qualquer matriz A de ordem $m \times n$ com entradas em R tem-se $A \circ J = A$;

- *Inversibilidade*: Seja $A = [a_{ij}] \in M_{m\times n}(R)$. 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 $\hat{A} = [\hat{a}_{ij}] = \left([a_{ij}^{-1}]\right)$. Além disso, vale que $A \circ \hat{A} = J$.

3.1 APLICAÇÃO EM CRIPTOGRAFIA

Definição (Dénes e Keedwell (1991)): Um *quadrado latino* é 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.

Observação: Para nosso trabalho, interessa apenas os quadrados latinos com entradas no conjunto dos números naturais (N).

Revista ARACÊ
ISSN: 2358-2472

Exemplo:

Figura 3

♣	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

Quadrado Latino.

♣	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Quadrado Latino.

♣	1	2	3
1	1	1	1
2	2	3	1
3	3	2	1

Não é Quadrado Latino.

Fonte: Autores.

Definição: Sejam $A, B \in M_n(N)$ e seja L um quadrado latino. Define-se a operação

$$A \odot_L B = L[a_{ij}, b_{ij}] \qquad (3)$$

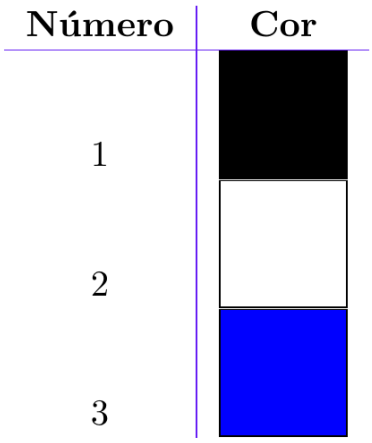
onde $L[a, b]$ representa a entrada na linha a e coluna b da matriz L.

Observação: A operação consiste em usar os pares (a_{ij}, b_{ij}) como coordenadas para consultar a matriz L.

Exemplo de atividade didática:

Consideremos a seguinte associação de cores e números:

Figura 4



Fonte: Autores.

Tarefa proposta: Construa uma matriz 3×3, utilizando apenas os números 1 e 2, com o objetivo de desenhar uma letra. Em seguida:

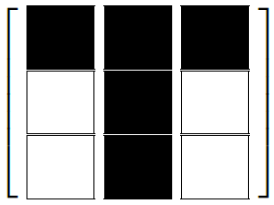
Revista ARACÊ
ISSN: 2358-2472

1. Crie uma matriz-chave (K) com números aleatórios menores ou iguais a 3;
2. Escolha um quadrado latino L qualquer, de ordem 3 x 3;
3. Aplique o processo de encriptação usando o quadrado L.

Possível solução de um aluno:

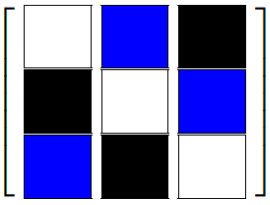
Figura 5

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

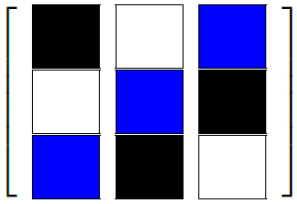


,

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



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



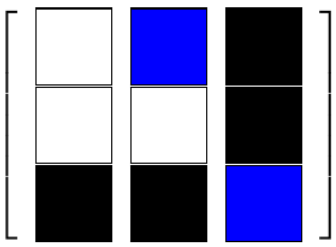
Fonte: Autores.

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

Figura 6

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

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



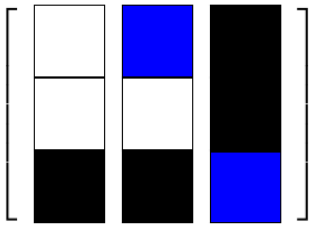
Fonte: Autores.

Revista ARACÊ
ISSN: 2358-2472

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:

Figura 7

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



Fonte: Autores.

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

O processo de decriptação 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 $m_{11} = 1 = PRETO$
- 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 $m_{12} = 1 = PRETO$
- 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 $m_{33} = 2 = BRANCO$.

O quadrado latino garante unicidade da descriptografia, o que assegura a reversibilidade do sistema. Enquanto embaralhar dados pode ser trivial, a criptografia exige que o processo seja sistemático e invertível. Essa é a função do quadrado latino no método. Na prática pedagógica, é possível destacar aos alunos que:

- o quadrado latino não precisa ser sigiloso;
- pode ser utilizado para mensagens diferentes;
- quadrados de ordem maior permitem imagens com mais cores e maior detalhamento;
- a operação combina ideias de funções, matrizes, estruturas algébricas e lógica computacional.

Assim, o sistema proposto articula conceitos elementares da Álgebra Linear com objetos discretos, apresentado aos estudantes uma aplicação concreta e contemporânea da matemática no conteúdo da criptografia.

Revista ARACÊ
ISSN: 2358-2472

4 CONCLUSÃO

O trabalho investigou o potencial do Produto de Hadamard como recurso pedagógico para o ensino de conceitos matemáticos e criptográficos, relacionando sua aplicação com contextos históricos e práticos da criptografia. A análise bibliográfica revelou a ausência dessa operação em produções acadêmicas nacionais, especialmente no PROFMAT, embora sua presença seja verificada em pesquisas internacionais, ainda que em níveis mais avançados de ensino. Essa lacuna reforça a necessidade de ampliar as discussões sobre operações matriciais alternativas no contexto da Educação Básica.

A proposta desenvolvida, apresentada por meio de uma sequência didática, mostrou que o Produto de Hadamard pode ser abordado de forma acessível no Ensino Básico. A aplicação em criptografia de imagens permitiu aproximar os estudantes de situações reais e contemporâneas, fortalecendo a aprendizagem de conceitos matriciais ao mesmo tempo em que promove motivação, contextualização e integração com as competências previstas pela BNCC. Assim, conteúdos tradicionalmente abstratos passam a adquirir sentido.

Pensando em desdobramentos futuros, destacamos que existe um sistema criptográfico matricial amplamente conhecido: a Cifra de Hill. Nesse método, letras são convertidas em números e, por meio do produto usual de matrizes, ocorre o embaralhamento desses valores. Esse embaralhamento é realizado pela multiplicação por uma matriz-chave, cuja inversa permite desfazer o processo, possibilitando a desencriptação da mensagem. Em nosso trabalho aplicamos o sistema ao embaralhamento de números e pixels associados a eles. A partir dessa perspectiva, abre-se a possibilidade de estender o método também ao tratamento de caracteres, como letras do alfabeto ou outros símbolos — de maneira análoga ao que se faz na Cifra de Hill.

Conclui-se, portanto, que os objetivos foram alcançados: o Produto de Hadamard mostra-se viável como ferramenta de ensino, reforçando a importância de integrar conteúdos matemáticos a situações contemporâneas e significativas. Além disso, abre-se espaço para novas pesquisas e aplicações didáticas que ampliem a presença da criptografia no contexto educacional brasileiro.

AGRADECIMENTOS

Este trabalho foi parcialmente suportado pela Fundação de Apoio à Pesquisa do Estado da Paraíba (FAPESQ-PB), com recursos oriundos do Edital nº 11/2023 – Concessão de Bolsas de Mestrado e Doutorado Profissional.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

BATISTA, A. G.; FONSECA, L. F. G. Criptografia no Ensino Básico. Revista FOCO: Interdisciplinary Studies. v.18, n.2, p. 01-21. 2025

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.

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Disponível em: https://basenacionalcomum.mec.gov.br. Acesso em: 1 jul. 2025.

BRASIL. Ministério da Educação. Secretaria de Educação Básica. Computação: complemento à BNCC. Brasília: MEC/SEB, 2022. Acesso em: 1 jul. 2025.

BRUXELAS, Ana Catarina. Aritmética modular e aplicações: criptografia RSA e calendário perpétuo. 2017. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2017.

COUTINHO, S. C. Criptografia. Rio de Janeiro: IMPA, 2016. 217 p. ISBN 978-85-244-0340-8.

DÉNES, J.; KEEDWELL, A. D. Latin squares and their applications. New York: Academic Press, 1991. ISBN 9780122091309.

DONIAK, M. H. Estudo da transformada de Walsh-Hadamard aplicada à transmissão OFDM. 2006. Tese (Doutorado em Engenharia Elétrica) – Universidade Federal de Santa Catarina, Centro Tecnológico, Florianópolis, 2006.

GLISTER, P. Digital literacy. New York: John Wiley & Sons, 1997.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). Em 2023, 87,2% das pessoas com 10 anos ou mais utilizaram internet. 2024. Publicado em 19 mar. 2024. 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. Acesso em: 1 jul. 2025.

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.

MILLION, Elizabeth. The Hadamard Product. 2007. Disponível em: http://buzzard.ups.edu/courses/2007spring/projects/million-paper.pdf. Acesso em: 8 set. 2025.

Resolução CNE/CEB nº 1/2022. Normas sobre Computação na Educação Básica – Complemento à BNCC. Diário Oficial da União, 6 out. 2022.

ROSSETO, Cintia Kohori. Criptografia como recurso didático: uma proposta metodológica aos professores de matemática. 2018. 84 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Estadual Paulista “Júlio de Mesquita Filho”, Instituto de Biociências, Letras e Ciências Exatas, São José do Rio Preto, 2018.

Revista ARACÊ
ISSN: 2358-2472

SILVA, Joaquim Denilson de Souza. Produto de Hadamard, criptografia e suas aplicações didático-conceituais no ensino básico. 2025. 111 f. Dissertação (Mestrado Profissional em Matemática – PROFMAT) – Universidade Federal de Campina Grande, Paraíba, 2025.

SILVA, Evelyn Gomes da. Criptografia RSA: da teoria à aplicação em sala de aula. 2019. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2019.

SINGH, Simon. O livro dos códigos: a ciência do sigilo, da Antiguidade à Era Quântica. Tradução de Vera Ribeiro. 8. ed. Rio de Janeiro: Record, 2013.

THEODORSON, George A.; THEODORSON, Achilles G. Modern Dictionary of Sociology. New York: Thomas Y. Crowell Company, 1969.

WIKIPÉDIA. Cítala. Disponível em: https://pt.wikipedia.org/wiki/Cítala. Acesso em: 3 dez. 2025.

Resolução CNE/CEB nº 1/2022. Normas sobre Computação na Educação Básica – Complemento à BNCC. Diário Oficial da União, 6 out. 2022.