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

Joaquim Denilson de Souza Silva

Produto Educacional

Entre Códigos e Matrizes: Ensino de Matemática com Criptografia e Produto de Hadamard

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

Entre Códigos e Matrizes: Ensino de Matemática com Criptografia e Produto de Hadamard

Produto Educacional vinculado ao 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

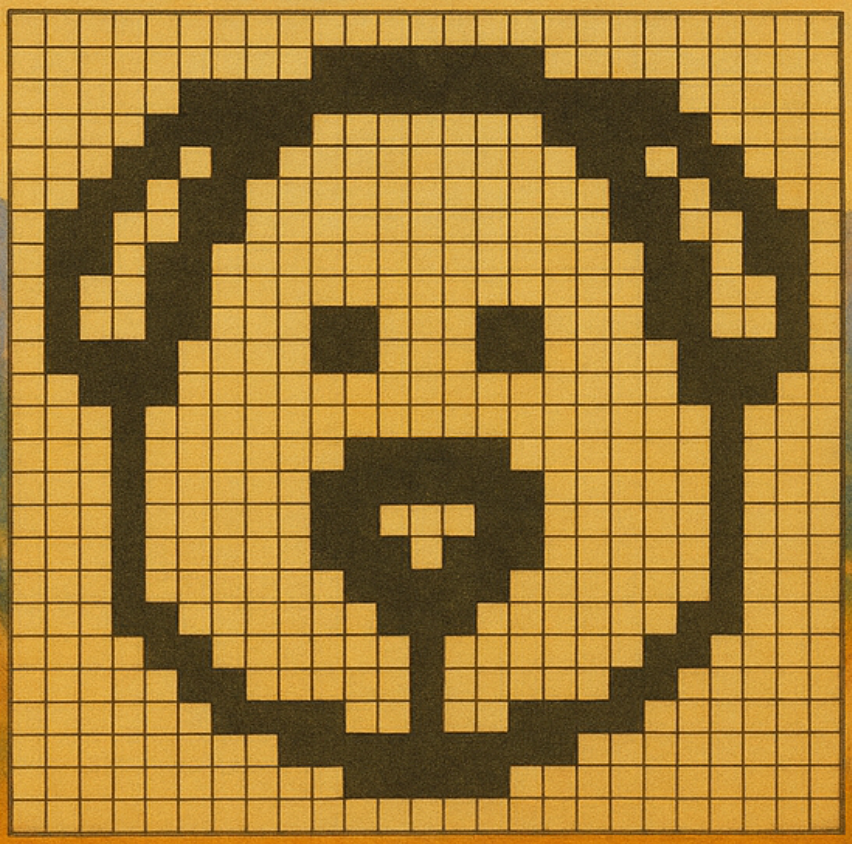
Campina Grande - PB
Agosto/2025

$$a \equiv b \pmod{m}$$

$$\begin{matrix} 0 & \boxed{1} \\ \boxed{1} & 0 \end{matrix}$$

$$f(x) = \pi^{\pi^{\pi}}$$

$$0 \times 1 = 0$$



Resumo

Este Produto Educacional apresenta uma proposta de atividade voltada para o Ensino Fundamental II e Médio, baseada no uso da criptografia como ferramenta de ensino da Matemática. A proposta parte de fundamentos biológicos e históricos da linguagem, contextualizando a curiosidade humana por segredos como um potente motivador para a aprendizagem. A sequência inclui atividades com cifras clássicas, como a cifra de César e o sistema espartano, além da introdução do Produto de Hadamard como recurso matemático para codificação. As atividades foram elaboradas com base na Educação Matemática Realística, na Modelagem Matemática e nos princípios da BNCC, buscando promover uma aprendizagem significativa, crítica e contextualizada. O material é voltado para professores que desejam tornar suas aulas mais contextualizadas, despertando o interesse dos estudantes por meio de temas instigantes e promovendo a aprendizagem significativa alinhada às competências contemporâneas da educação básica.

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

Abstract

This Educational Product presents a activity proposal designed for lower and upper secondary education, based on the use of cryptography as a tool for teaching Mathematics. The proposal is grounded in biological and historical aspects of language, framing human curiosity about secrets as a powerful motivator for learning. The sequence includes activities with classical ciphers, such as the Caesar cipher and the Spartan scytale, as well as the introduction of the Hadamard Product as a mathematical resource for encoding. The activities were developed within the frameworks of Realistic Mathematics Education, Mathematical Modeling, and the principles of the Brazilian National Common Core (BNCC), aiming to promote meaningful, critical, and contextualized learning. This material is intended for teachers who seek to make their classes more connected to students' realities, awakening interest through engaging themes and fostering meaningful learning aligned with contemporary educational competencies.

Keywords: Hadamard Product; Cryptography; Mathematics Education.

1 Introdução

O presente Produto Educacional propõe a utilização de atividades didáticas baseadas na criptografia como estratégia para desenvolver competências matemáticas no Ensino Fundamental II e Ensino Médio. A escolha desse tema se fundamenta na constatação de que a aprendizagem se torna mais significativa quando vinculada a contextos instigantes, capazes de mobilizar a curiosidade e o envolvimento ativo dos estudantes.

As atividades elaboradas têm como inspiração as raízes biológicas e históricas do desejo humano de compartilhar e proteger informações. A proposta foi estruturada de modo a contemplar diferentes níveis de complexidade e conexão com os conteúdos previstos pela Base Nacional Comum Curricular (BNCC), assim como pelo documento complementar que trata da Computação na Educação Básica.

O presente trabalho foi desenvolvido com o apoio financeiro da Fundação de Apoio à Pesquisa do Estado da Paraíba - FAPESQ.

2 Fundamentação

2.1 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, 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 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.

3 Atividades didáticas

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), enquanto Falcón et al. (2023) serviu de base para a atividade sobre o Produto de Hadamard. As atividades aqui exploradas podem ser consultadas com mais profundidade em Silva (2025), trabalho realizado por mim para a obtenção do título de mestre, de onde se deriva este produto educacional.

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.

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.

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.

3.4 Atividade 1 – Cifra de César: Alerta ao Aliado

Ilustração:

Figura 1 – 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.

3.4.1 Atividade 2 – Cítale Espartano: O dia do amigo

Instrução visual:

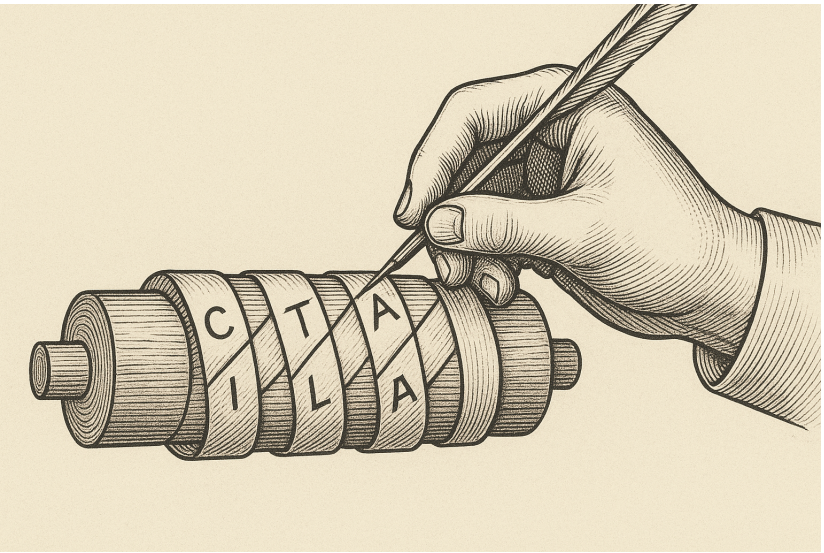


Figura 2 – Exemplificação de construção do Cítale Espartano

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.

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

Ilustração:

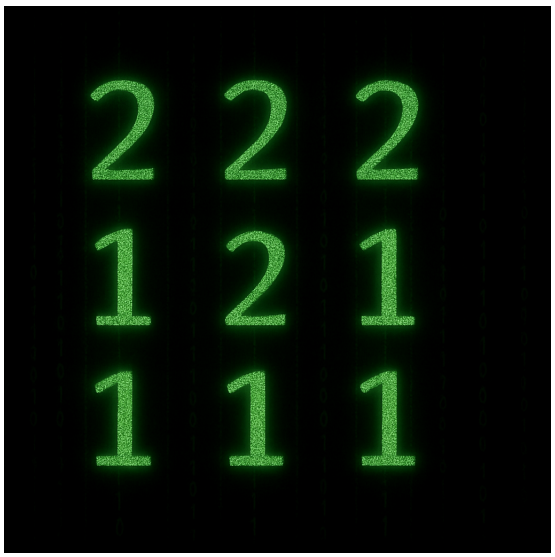


Figura 3 – "MatriX"

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, onde:

Definição 3.1. *Sejam A e B matrizes de ordem n com entradas em $\mathbb{N}$, e seja L um quadrado latino de ordem n. Define-se a operação*

$$(A \odot_L B)[i,j] = L[A[i,j], B[i,j]] \tag{3.1}$$

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 $i,j \in \mathbb{N}$.

Logo:

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

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.

4 Conclusões

O desenvolvimento deste Produto Educacional buscou demonstrar que a utilização de temas instigantes, como a criptografia, pode transformar a maneira como a Matemática é percebida pelos estudantes, tornando-a mais próxima, curiosa e significativa. Ao propor atividades que envolvem códigos secretos, narrativas de mensagens sigilosas e a modelagem de situações reais, pretende-se promover uma aprendizagem que ultrapassa a mera memorização de procedimentos, estimulando a investigação, o raciocínio lógico e o trabalho colaborativo.

Espera-se que este material, que consiste em parte de minha dissertação de mestrado, seja semente geradora de novos interesses no alunado contemporâneo, contribuindo para a matearização dos conteúdos estudados em matemática e despertando interesse por novas áreas de conhecimento, como a criptografia e suas aplicações em programação.

Por fim, recomenda-se que as atividades aqui apresentadas sejam adaptadas conforme a realidade de cada turma e que sejam acompanhadas de momentos de reflexão ética sobre o uso das informações e das técnicas de codificação, ampliando a compreensão dos estudantes sobre os impactos da criptografia na sociedade.

Referências

Base Nacional Comum Curricular. *Base Nacional Comum Curricular*. Brasília: Ministério da Educação, 2018. Disponível em: <https://basenacionalcomum.mec.gov.br/>. Citado 2 vezes nas páginas 6 e 14.

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 na página 8.

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 2 vezes nas páginas 6 e 7.

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 na página 8.

SILVA, J. D. d. S. *Produto de Hadamard, Criptografia e Suas Aplicações Didático-Conceituais no Ensino Básico*. Dissertação (Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT)) — Universidade Federal de Campina Grande, Campina Grande, Aug 2025. Citado na página 8.

SINGH, S. *O livro dos códigos*. [S.l.]: Editora Record, 2001. Citado na página 8.