Revista Even. Pedagóg.
Número regular – O ensino de matemática e os cotidianos escolares
Sinop, v. 16, n. 3 (43. ed.), p. 1016-1039, nov./dez. 2025
ISSN 2236-3165 | DOI: 10.30681/2236-3165
https://periodicos.unemat.br/index.php/reps

CRIPTOGRAFIA NA SALA DE AULA:

estratégias para o ensino de matemática através de códigos e cifras[1]

CRYPTOGRAPHY IN THE CLASSROOM:

strategies for teaching mathematics through codes and ciphers

Isac Rosa Rodrigues [i]

Luciana Assis [ii]

Raul Abreu de Assis [iii]

RESUMO: Este artigo apresenta um material de apoio para professores do 9º ano do Ensino Fundamental II, composto por duas atividades baseadas em técnicas de criptografia para explorar conteúdos como divisão euclidiana, aritmética modular, progressões aritméticas e operações matriciais. As propostas também podem ser aplicadas no Ensino Médio. Fundamentado na Aprendizagem Significativa e na Aprendizagem Baseada em Projetos, o estudo descreve o desenvolvimento e a aplicação das atividades em sala. Os resultados indicam maior engajamento dos estudantes e melhor compreensão conceitual. Conclui-se que a criptografia torna o ensino de Matemática mais contextualizado, motivador e alinhado à Base Nacional Comum Curricular.

Palavras-chave: Aprendizagem significativa. Aprendizagem baseada em projetos. Técnicas criptográficas.

ABSTRACT: This article presents support material for 9th-grade teachers in lower secondary education, consisting of two activities based on cryptography techniques to explore mathematical topics such as Euclidean division, modular arithmetic, arithmetic progressions, and matrix

[1] Este texto tem origem em uma pesquisa de Mestrado desenvolvidas no âmbito do Programa de Pós-graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Campus Universitário de Sinop da Universidade do Estado de Mato Grosso (UNEMAT).

Este trabalho está licenciado sob CC BY-SA 4.0. Para ver uma cópia desta licença, visite:
https://creativecommons.org/licenses/by-sa/4.0/deed.pt_BR

operations. The proposals can also be applied in high school. Grounded in Meaningful Learning and Project-Based Learning, the study describes the development and classroom implementation of the activities. The results indicate increased student engagement and improved conceptual understanding. It is concluded that the use of cryptography makes Mathematics teaching more contextualized, motivating, and aligned with the Brazilian National Common Curriculum Base.

Keywords: Meaningful learning. Project-based learning. Cryptographic techniques.

1 INTRODUÇÃO

A Matemática se faz presente de diferentes maneiras em nosso cotidiano, permeando as atividades mais sutis de nosso dia a dia, desde a gestão de finanças pessoais até a resolução de problemas práticos, como calcular trajetórias ou dimensionar receitas na cozinha. No entanto, a maneira como a Matemática é tradicionalmente ensinada nas escolas, frequentemente diverge dessa realidade cotidiana levantando questões pertinentes sobre a sua eficácia na formação dos alunos.

O distanciamento entre a aplicação prática da Matemática e seu ensino formal, tem sido objeto de estudo e reflexão em diversas obras acadêmicas. Freire (1973), aponta que práticas pouco conectadas à realidade dos estudantes podem comprometer o engajamento e a compreensão conceitual. Segundo esse autor, "A educação só ganha sentido quando está enraizada na realidade concreta dos educandos; quando a desconsidera, transforma-se em algo estranho e distante, que pouco contribui para sua formação" (Freire, 1973, p. 39).

Outros autores como Ball (1990) e Boaler (2016), também exploraram as lacunas entre a vivência matemática do indivíduo e o currículo escolar.

Segundo Ball (1990), "Quando os conceitos matemáticos são ensinados como procedimentos isolados, desconectados de contextos significativos, os alunos frequentemente não conseguem desenvolver uma compreensão sólida desses conceitos" (Tradução de: Ball, 1990, p. 454).

Já Boaler (2016) afirma que "Os alunos perdem o interesse quando a matemática é apresentada como um conjunto de regras a serem memorizadas, em vez de um conjunto significativo de ideias conectadas ao mundo real" (Boaler, 2016, p. 24).

Nesse cenário, práticas pedagógicas que favoreçam a participação ativa e a aprendizagem significativa tornam-se essenciais. Dessa forma, este estudo fundamenta-se na teoria da Aprendizagem Significativa, de Ausubel (1968), e na Aprendizagem Baseada em Projetos (ABP), apoiada em autores como Dewey (1979), Vygotsky (1978) e Thomas (2000). Esses referenciais destacam o papel do conhecimento prévio, da mediação docente e das situações reais de aprendizagem para a construção de significados. Para Vygotsky (1978), "O aprendizado desperta diversos processos internos de desenvolvimento que só podem ocorrer quando a criança interage com outras pessoas, em cooperação e em um ambiente socialmente mediado" (Vygotsky, 1978, p. 90).

Dessa forma, "a aprendizagem só ocorre de maneira efetiva quando ligada à experiência; separar a escola da vida e dos problemas reais é tornar o conhecimento algo vazio de significado" (Dewey, 1979, p. 77).

Um ponto importante sobre a relevância desse trabalho, está em oferecer a professores do Ensino Fundamental II e do Ensino Médio um conjunto de estratégias capazes de tornar o ensino de Matemática mais acessível, contextualizado e motivador. O uso de técnicas de criptografia, como o citale, a multiplicação de matrizes e as cifras de transposição, constitui uma abordagem que promove investigação, pensamento lógico e aplicação prática de conceitos matemáticos previstos na Base Nacional Comum Curricular (BNCC) (Brasil, 2017).

O objetivo geral deste estudo é apresentar um conjunto de atividades baseadas em criptografia que favoreçam o trabalho contextualizado e interdisciplinar de conteúdos matemáticos no Ensino Fundamental II e no Ensino Médio. De maneira mais específica, buscamos relacionar técnicas criptográficas com conteúdos matemáticos, como divisão euclidiana, aritmética modular, progressões aritméticas, matrizes, permutações e análise combinatória. Além disso, descrever o desenvolvimento e a aplicação das atividades em sala de aula, fundamentando-as em teorias sobre aprendizagem, de modo que seja possível evidenciar como as propostas dialogam com habilidades e competências da BNCC. Por fim, analisamos as potencialidades pedagógicas das atividades, especialmente no que se refere ao engajamento dos estudantes e ao favorecimento de aprendizagens significativas.

Por fim, a estrutura deste artigo organiza-se da seguinte forma: a Seção 2 apresenta os referenciais teóricos; a Seção 3 descreve as atividades propostas; e a Seção 4 apresenta as reflexões finais sobre o potencial pedagógico da abordagem.

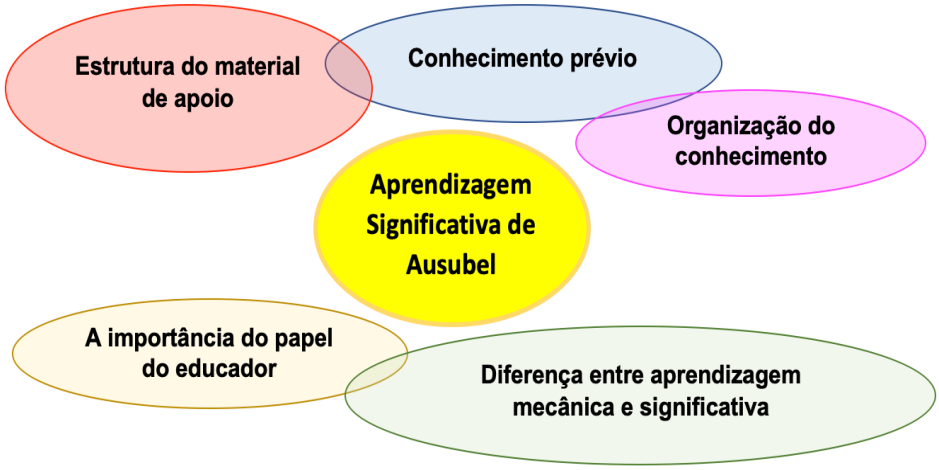
2 APORTES TEÓRICOS

Nesta Seção, apresentamos uma revisão sobre Aprendizagem Significativa e Aprendizagem Baseada em Projetos (ABP) que servirão para fundamentar a proposta de atividades. Além disso, relacionamos as habilidades da BNCC com os conteúdos matemáticos abordados em nossa proposta de atividades que foram elaboradas especialmente para os alunos Ensino Fundamental II e do Ensino Médio.

2.1 Aprendizagem significativa

A Aprendizagem Significativa é uma teoria da aprendizagem proposta pelo psicólogo educacional David Ausubel, que enfatiza a importância em conectar novos conhecimentos com o conhecimento prévio do aprendiz (Ausubel, 1968). De acordo com Ausubel (1968), existem alguns pontos essenciais no processo de aprendizagem que devem ser explorados, na Figura 1, fazemos um esboço de tais pontos, os quais detalhamos em seguida.

Figura 1 - Pontos essenciais no processo de aprendizagem que devem ser explorados (Ausubel, 1968).



Fonte: elaborado pelos autores (2025).

Para o autor, o conhecimento prévio é considerado algo fundamental para uma aprendizagem significativa, já que o conhecimento é ancorado em conceitos, ideias e informações já existentes ou conhecidas (Ausubel, 1968, p. 44). Além disso, é necessário que ocorra a organização do conhecimento, para que o processo de ensino e de aprendizagem seja efetivo, ou seja, é essencial que o aprendizado comece com conceitos mais gerais para depois progredir para conceitos mais específicos (Ausubel, 1968, p. 148). Isso facilita a compreensão e a retenção do novo conhecimento.

Há ainda, a diferença entre aprendizagem mecânica e aprendizagem significativa, onde na aprendizagem mecânica o conhecimento é memorizado de forma superficial, muitas vezes sem compreensão real, podendo ser esquecido rapidamente. Por outro lado, na aprendizagem significativa, os novos conceitos são incorporados de forma lógica e integrados ao conhecimento prévio do aprendiz. Isso torna o aprendizado mais prático e útil, uma vez que o aluno é capaz de aplicar o conhecimento em contextos diversos (Ausubel, 1968, p. 160).

Em relação à estrutura do material de apoio, (Ausubel, 1968, p. 260) enfatiza que, ao se projetar materiais de apoio, estes devem ser claros e organizados, respeitando a organização do conhecimento em estudo, ajudando os alunos a conectarem o novo conhecimento com o que já sabem.

Finalmente, não podemos deixar de citar a importância do papel do educador, já que este auxilia os alunos a identificar e organizar seus conhecimentos prévios, criando conexões relevantes entre os conceitos e cultivando a reflexão. Dessa forma, os educadores devem adaptar suas abordagens de ensino de acordo com as necessidades e níveis de compreensão de cada aluno (Ausubel, 1968, p. 425).

De maneira resumida, a Aprendizagem Significativa destaca a importância de se construir o conhecimento a partir do que já sabemos, em oposição à mera memorização de fatos isolados. Essa abordagem visa possibilitar ao aprendiz uma análise crítica e organizada dos conceitos estudados, além da capacidade de deduzir e demonstrar conceitos novos e relações a partir do conhecimento que já foi incorporado, criando assim uma base sólida de compreensão que os alunos possam aplicar em diversas situações, promovendo uma aprendizagem mais rigorosa e útil.

2.2 Aprendizagem baseada em projetos (ABP)

A Aprendizagem Baseada em Projetos (ABP) é uma abordagem pedagógica que tem ganhado destaque no ambiente educacional contemporâneo.

Segundo Thomas (2000), a ABP envolve a investigação de problemas complexos e desafiadores, frequentemente interdisciplinares, por meio da elaboração e execução de projetos, o que favorece uma aprendizagem mais contextualizada e significativa (Thomas, 2000, p. 1–2).

Nesse contexto, Dewey (1979) afirma que o aprendizado se dá quando o aluno participa de "atividades intencionais" que envolvem investigação, experimentação e resolução de problemas (p. 157–158). Ele destaca a importância de experiências práticas e concretas para a construção do conhecimento, apontando que a realização de projetos envolve os alunos em um processo ativo de aprendizagem (p. 143).

Além disso, Vygotsky (1978) desenvolveu o conceito de Zona de Desenvolvimento Proximal (ZDP), que descreve a diferença entre o que um aluno pode fazer sozinho e o que pode fazer com a ajuda de outras pessoas. A ABP promove exatamente esse tipo de interação social e colaboração, ao incentivar os alunos a resolver problemas de forma ativa e colaborativa, com o apoio de colegas ou facilitadores. (Vygotsky, 1978, p. 84). Dessa forma a ABP oferece oportunidades para a construção do conhecimento em um contexto social, onde os alunos interagem, colaboram e negociam significados, contribuindo para o desenvolvimento cognitivo e socioemocional.

A criação de projetos alinhados aos objetivos de aprendizagem e a adaptação às necessidades dos alunos são aspectos cruciais para o sucesso dessa abordagem. Devemos ainda, considerar o fato de que, projetos costumam envolver diferentes áreas do saber. Dessa forma, a ABP pode ser aplicada para se tratar não apenas conteúdos de disciplinas isoladas do currículo, mas também os chamados temas transversais definidos pela BNCC como essenciais de serem abordados no Ensino Fundamental II e no Ensino Médio.

2.3 Ensino de Matemática

O Ensino de Matemática é um desafio constante para educadores, exigindo estratégias e intervenções pedagógicas eficazes para promover uma aprendizagem significativa e engajadora. Segundo a Base Nacional Curricular Comum (BNCC) a Matemática, como disciplina escolar, deve ser apresentada de forma contextualizada, estimulando a compreensão e a aplicação dos conceitos no cotidiano dos alunos como ferramentas para a compreensão dos mundos mental, social e natural (Brasil, 2017, p. 253).

Para atender a essa demanda, é essencial adotar metodologias que estimulem a participação ativa dos estudantes no processo de aprendizagem. Nesse sentido, Oliveira (2016) destaca a importância de estratégias como a resolução de problemas, o uso de jogos educativos e a manipulação

de materiais concretos como meios experimentais para desenvolver o raciocínio lógico-matemático dos alunos. A resolução de problemas, de acordo com Fiorentini e Lorenzato (2006), permite aos alunos aplicar os conhecimentos matemáticos em situações reais, estimulando o pensamento crítico e a busca por soluções. Além disso, o uso de jogos educativos, conforme recomendações de D'ambrósio (1996), proporciona um ambiente lúdico e motivador, promovendo uma aprendizagem por meio do prazer e da interação social.

A manipulação de materiais concretos, como defendido por Castellar (2014), é uma estratégia eficaz para a compreensão de conceitos abstratos. O contato direto com objetos tangíveis possibilita aos alunos uma visualização mais clara e uma compreensão mais profunda dos conceitos matemáticos. Nesse contexto, o conceito de materiais concretos pode ser generalizado para o de situações concretas nas quais não necessariamente existe um objeto físico a ser medido ou de algum modo quantificado por meios matemáticos, mas sim situações onde se faz necessária uma análise quantitativa, organizada e logicamente fundamentada para a resolução de algum problema característico da situação, podendo então ser feito o uso de ferramentas matemáticas para a compreensão da natureza da situação, dedução de suas propriedades, elaboração de hipóteses e de algoritmos para resolução de problemas.

Nesse cenário, torna-se evidente que metodologias que promovem a participação ativa, a investigação e a resolução de problemas constituem caminhos promissores para tornar o ensino de Matemática mais significativo e conectado à realidade dos alunos. Ao buscar estratégias que integrem conceitos abstratos a situações práticas e desafiadoras, amplia-se o potencial de engajamento e compreensão dos estudantes. É nesse contexto que a criptografia surge como uma alternativa pedagógica particularmente pertinente, possibilitando a exploração de conceitos matemáticos por meio de desafios autênticos e atividades investigativas.

A criptografia, ao longo da história humana, desempenhou um papel crucial na proteção de informações sensíveis e na garantia da segurança de comunicações em diversos contextos. Maiores detalhes sobre o desenvolvimento da criptografia poder ser encontrada em Rodrigues (2024). Seu uso no ensino de Matemática tem se mostrado uma metodologia promissora para motivar os alunos e tornar o processo de aprendizagem mais interativo e aplicável. Embora a criptografia seja associada à segurança da informação, no contexto educacional seu potencial vai além, permitindo que os alunos aprendam conceitos matemáticos de forma prática, como em problemas de codificação e decodificação de mensagens.

No Ensino Médio, por exemplo, a criptografia tem sido utilizada como ferramenta didática, especialmente para o ensino de conteúdos como combinatória e álgebra. Um estudo empírico realizado por Vidal *et al.* (2022) aplicou uma sequência didática para ensinar análise combinatória por meio da criptografia. A sequência envolveu 26 horas de aula e foi implementada em uma turma de 22 alunos do segundo ano do Ensino Médio. A proposta incluiu técnicas de contagem e conceitos criptográficos, como a cifra de César e a criptografia binária, além de conexões com a criptografia apresentada no filme O Código Da Vinci. Pontes *et al.* (2022) exploraram o uso de funções polinomiais na criptografia como uma prática pedagógica inovadora para alunos do final do Ensino Fundamental e início do Ensino Médio. A abordagem consistiu em codificar e decodificar mensagens usando

polinômios, o que permite que os alunos compreendam melhor a álgebra e suas aplicações em situações reais, promovendo maior engajamento e motivação para o aprendizado de Matemática.

Outro exemplo de integração da criptografia no Ensino Médio pode ser observado no uso de criptografia para ensinar matrizes. A proposta de usar matrizes como parte de um sistema criptográfico não só auxilia na compreensão do conceito, como também fornece uma aplicação concreta para uma área abstrata da Matemática (Melo, 2014).

Além das abordagens tradicionais, a criptografia também se beneficia do uso de tecnologias digitais como ferramentas complementares no ensino. Silva *et al.* (2022) propõem que o uso de softwares criptográficos aliados à tecnologia digital pode aumentar o interesse dos alunos pela Matemática, proporcionando uma interface interativa para aprender conceitos matemáticos complexos de maneira mais intuitiva e acessível.

2.4 Habilidades da BNCC

As atividades propostas neste trabalho estão relacionadas com algumas habilidades da Base Nacional Comum Curricular (BNCC) para os Ensinos Fundamental II e Médio na área de Matemática e suas tecnologias. A seguir, apresentamos no Quadro 1, algumas das habilidades da BNCC contempladas e como elas se relacionam com a proposta de atividades elaboradas em nossa pesquisa.

Quadro 1 - Habilidades da BNCC que contemplam a proposta de atividades.

Habilidades da BNCC	Relação com a proposta de atividades
(EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.	Os conceitos de múltiplos e de divisores estão fortemente relacionados com a divisão euclidiana na forma de quociente e resto. O caso particular em que o resto de uma divisão é zero pode ser utilizado para definir tais conceitos. Para isso utilizamos a técnica de criptografia utilizando um *citale*, em que os múltiplos e divisores aparecem naturalmente como uma forma de técnica de decifragem.
(EF09MA03) Efetuar cálculos com números reais, inclusive potências com expoentes fracionários.	As diversas atividades propostas envolvem a realização das operações básicas com números reais, mesmo que a fim de focar nas ideias utilizadas e não nas operações os exemplos foram elaborados em sua maioria utilizando números inteiros.
(EM13MAT102) Analisar tabelas, gráficos e amostras de pesquisas estatísticas apresentadas em relatórios divulgados por diferentes meios de comunicação, identificando, quando for o caso, inadequações que possam induzir a erros de	A habilidade de criar, analisar e manipular gráficos e tabelas é frequentemente necessária para lidar com as transformações e permutações pelas quais os caracteres de um texto passam durante uma cifragem.

interpretação, como escalas e amostras não apropriadas.	
(EM13MAT301) Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais.	Sistemas lineares de equações podem ser representados na forma matricial e a solução pode ser obtida através de operações matriciais, entre elas o cálculo do determinante da matriz que também é utilizado na cifragem por multiplicação de matrizes para determinar se uma matriz é invertível ou não.
(EM13MAT302) Construir modelos empregando as funções polinomiais de 1º ou 2º graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais.	Na atividade da cifragem por citale podemos modelar a posição de um caractere do texto original no texto cifrado como função da sua posição no texto original através de uma função afim onde o número de lados do citale é o coeficiente angular e a posição de uma letra arbitrária no texto cifrado através da qual indicamos a posição dos outros caracteres é o coeficiente linear.
(EM13MAT310) Resolver e elaborar problemas de contagem envolvendo agrupamentos ordenáveis ou não de elementos, por meio dos princípios multiplicativo e aditivo, recorrendo a estratégias diversas, como o diagrama de árvore.	As técnicas de contagem e aplicação dos princípios aditivo e multiplicativo são ferramentas usadas para definir o número de cifras distintas que podemos obter ao aplicar determinado tipo de cifragem.
(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.	Na cifragem por citale o número de lados do citale utilizado para cifrar um texto define a razão de um conjunto de progressões aritméticas que podem ser usadas para identificar quais números deixam o mesmo resto ao serem divididos por um mesmo divisor.

Fonte: elaborado pelos autores a partir de (Brasil, 2017).

Essas habilidades da BNCC evidenciam a relevância e a aplicabilidade das atividades propostas, pois estão diretamente relacionadas à resolução de problemas, interpretação de situações-problema, aplicação de conceitos matemáticos em diferentes contextos e desenvolvimento do pensamento crítico e analítico dos alunos. Além das habilidades citadas, em geral, as habilidades da BNCC concentram-se na capacidade de resolução de problemas e aplicações práticas da matemática, o que evidentemente é abordado neste trabalho.

3 METODOLOGIA

Este estudo caracteriza-se como uma pesquisa qualitativa, de natureza aplicada e caráter descritivo, voltada à elaboração e análise de atividades de criptografia para o ensino de Matemática. A metodologia foi organizada em três etapas.

Na primeira etapa, foram desenvolvidas duas atividades baseadas em técnicas de criptografia por meio do citale e de operações matriciais, alinhadas às habilidades da BNCC e fundamentadas nos referenciais da Aprendizagem Significativa (Ausubel, 1968) e da Aprendizagem Baseada em Projetos (Thomas, 2000; Dewey, 1979). A elaboração considerou o conhecimento prévio dos alunos e o potencial investigativo das tarefas.

Na segunda etapa, as atividades foram aplicadas em turmas do 9º ano e do Ensino Médio. As aulas ocorreram de forma presencial e envolveram trabalho em grupo, manipulação de materiais concretos e uso de recursos digitais. Durante a aplicação, foram registrados aspectos como participação dos alunos, estratégias de resolução e principais dificuldades.

Na terceira etapa, realizou-se uma análise qualitativa das observações e produções dos estudantes, buscando identificar evidências de engajamento, compreensão dos conceitos matemáticos e potencial da criptografia como recurso didático. A análise permitiu avaliar a pertinência das propostas como ferramenta para tornar o ensino mais contextualizado e motivador.

Embora tenhamos considerado o conhecimento prévio dos alunos e o potencial investigativo das tarefas, além de registrar aspectos como a participação dos alunos e ainda avaliar a pertinência das propostas, optamos neste trabalho, por apresentar a sequência de atividades para que outros docentes possam aplicar junto aos seus alunos. Detalhes sobre tais aspectos metodológicos podem ser encontrados em Rodrigues (2024).

4 PROPOSTA DE ATIVIDADES PARA O ENSINO BÁSICO

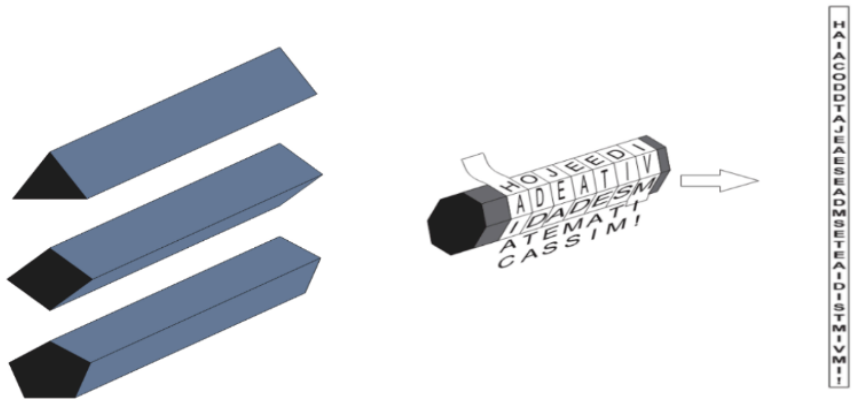
4.1 Proposta de atividades para o Ensino Básico

As atividades propostas foram trabalhadas em turmas do 9º ano do Ensino Fundamental II e também em turmas do Ensino Médio. Nosso propósito é apresentar as atividades para que outros professores possam aplicar em suas salas de aula.

4.1.1 Atividade 1: Cifrar e decifrar mensagens por meio de citales para fixação dos conteúdos divisão euclidiana, aritmética modular e progressão aritmética.

Um citale é um prisma cuja base é um polígono regular conforme ilustrado na Figura 2. Ao redor de suas faces retangulares enrolamos uma tira de papel ou outro material para escrita e escrevemos uma mensagem ao longo do eixo longitudinal do citale, na qual desejamos cifrar. Em geral, omitimos espaços, acentuações e pontuações para que haja mais eficiência na cifragem.

Figura 2 - Citales e o funcionamento da cifra do citale.



Fonte: elaborado pelos autores (2025).

Quando desenrolamos a tira de papel, as letras ficam embaralhadas, obtendo-se assim a mensagem cifrada. Letras consecutivas do texto original se encontrarão à uma mesma distância umas das outras no texto cifrado e, dessa maneira, se enumerarmos as letras no texto cifrado de acordo com sua posição, a divisão do número relativo à posição pelo número de lados da base do citale deixará o mesmo resto quando as letras em questão forem consecutivas no texto original.

Assim, a mensagem só pode ser lida quando enrolada no citale, ou então, passando por um processo de decifragem. Cada grupo recebeu uma nova mensagem cifrada fornecida por outro grupo utilizando citale de papel cartão fornecidos pelo professor e, para decifrar a mensagem sem ter informações sobre o número de lados de sua base os alunos tiveram que perceber o padrão no posicionamento das letras nas tiras.

Vejamos um exemplo de cifragem por meio de um citale. Considere a mensagem a ser cifrada, 'Hoje é dia de atividades matemáticas? Sim!', e em seguida, retire os caracteres de espaços, acentuações e pontuações transformando a mensagem em HOJEEDIADEATIVIDADESMATEMATICASSIM e, desse modo, ao desenrolar a tira de papel de um citale de cinco lados a mensagem cifrada será dada por HAIACODDTAJEAESEADMSETEAIDISTMIVMI (veja ilustração na Figura 3).

Figura 3 - Mensagem original, seguida da ausência caracteres (espaços, acentuações e pontuações), seguida da mensagem cifrada.

Fonte: elaborado pelos autores (2025).

Para simplificar o processo e a realização das atividades, os textos usados devem ser escritos de modo que ocupem por inteiro o último lado (chamaremos simplesmente de lado as faces retangulares do citale) utilizado do citale, ou seja, ou o número de caracteres do texto deve ser múltiplo do número de voltas dadas com a tira ao redor do citale, ou, ao final do texto, caso o último lado ocupado não tenha sido preenchido por completo, devemos inserir caracteres aleatórios até que todo espaço do último lado seja ocupado. As atividades propostas foram elaboradas considerando este critério de simplificação.

Devemos nos atentar para o fato de que não é obrigatório usar todos os lados do citale. No exemplo da Figura 3, usamos um citale cuja base é um polígono regular de 8 lados. Entretanto, como a mensagem é curta e só ocupou 5 desses lados, resultando espaços em branco na tira onde o texto da mensagem foi escrito. Isso fornece indício do número de lados do citale utilizado, podendo facilitar uma possível decifragem.

Para evitar tal fraqueza na cifragem é possível transcrever o texto cifrado para outro lugar eliminando-se os espaços em branco. Uma outra abordagem consiste em manter o texto da mensagem na tira, de forma que preenchemos os lados não ocupados pelo texto da mensagem com caracteres aleatórios que serão facilmente reconhecidos como um artifício de simples preenchimento de espaço por quem decifrar o texto da mensagem.

O método básico de decifragem do citale consiste em manter o texto na tira enrolando-a em um citale idêntico ao que foi usado para cifrar o texto. Porém existem outros métodos, usados quando o texto é transcrito para outro lugar ou quando não se conhece as características do citale usado para cifrar o texto.

Se observarmos a estrutura do citale, notaremos que as letras consecutivas no texto original estão a uma mesma distância umas das outras no texto cifrado. Assim, se numerarmos a posição de

cada letra no texto cifrado, a divisão do número relativo à posição de letras consecutivas no texto original pelo número de lados do citale (seja tanto o número total de lados como o número de lados efetivamente utilizados), deixará um mesmo resto, e assim, o texto poderá ser decifrado desde que identifiquemos o número de lados em questão.

Isso pode ser feito dividindo o número relativo à posição das letras no texto cifrado por algum número inteiro, agrupando aquelas cujos restos forem iguais e analisando se a sequência de letras obtidas faz algum sentido. Caso não faça, repetimos o processo atribuindo um outro número como divisor, repetindo até encontrarmos o divisor adequado.

Seguindo com nosso exemplo, numeramos os caracteres do texto cifrado (veja a Figura 4).

Figura 4 - Posição das letras no texto cifrado

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
H	A	I	A	C	O	D	D	T	A	J	E	A	E	S	E	A

18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
D	M	S	E	T	E	A	I	D	I	S	T	M	I	V	M	I

Fonte: elaborado pelos autores (2025).

Como o menor número possível de lados de um prisma é 3, iniciaremos com a divisão por 3, dos números relativos às posições das letras no texto cifrado. A Figura 5 apresenta a divisão euclidiana de cada número relativo c presente na Figura 4, cujo divisor é $b = 3$, o resto é r e o quociente é q, considerando $c = qb + r; 0 \leq r < b$.

Figura 5 - Aplicação da divisão euclidiana $c = qb + r; 0 \leq r < b$, em cada caractere presente no texto cifrado.

r \ c	H	A	I	A	C	O
$r = 1$	$1 = 0 * 3 + 1$			$4 = 1 * 3 + 1$		
$r = 2$		$2 = 0 * 3 + 2$			$5 = 1 * 3 + 2$	
$r = 0$			$3 = 1 * 3 + 0$			$6 = 2 * 3 + 0$

r \ c	D	D	T	A	J	E
$r = 1$	$7 = 2 * 3 + 1$			$10 = 3 * 3 + 1$		
$r = 2$		$8 = 2 * 3 + 2$			$11 = 3 * 3 + 2$	
$r = 0$			$9 = 3 * 3 + 0$			$12 = 4 * 3 + 0$

r \ c	A	E	S	E	A	D
$r = 1$	$13 = 4 * 3 + 1$			$16 = 5 * 3 + 1$		
$r = 2$		$14 = 4 * 3 + 2$			$17 = 5 * 3 + 2$	
$r = 0$			$15 = 5 * 3 + 0$			$18 = 6 * 3 + 0$

r \ c	M	S	E	T	E	A
$r = 1$	$19 = 6 * 3 + 1$			$22 = 7 * 3 + 1$		
$r = 2$		$20 = 6 * 3 + 2$			$23 = 7 * 3 + 2$	
$r = 0$			$21 = 7 * 3 + 0$			$24 = 8 * 3 + 0$

r \ c	I	D	I	S	T	M
$r = 1$	$25 = 8 * 3 + 1$			$28 = 9 * 3 + 1$		
$r = 2$		$26 = 8 * 3 + 2$			$29 = 9 * 3 + 2$	
$r = 0$			$27 = 9 * 3 + 0$			$30 = 10 * 3 + 0$

r \ c	I	V	M	I		
$r = 1$	$31 = 10 * 3 + 1$			$34 = 11 * 3 + 1$		
$r = 2$		$32 = 10 * 3 + 2$				
$r = 0$			$33 = 11 * 3 + 0$			

Fonte: elaborado pelos autores (2025).

Na Figura 5, considere c o caractere respeitando-se a ordem em que aparece na mensagem cifrada (ver Figura 4), r é o resto e q é o quociente na divisão de c por 3.

Como teste, vamos agrupar algumas letras correspondentes ao resto 1. Assim obtemos a sequência 1, 4, 7, 10, 13, 16 que corresponde a sequência de letras ADDAAE. Como a sequência parece não fazer muito sentido, testaremos o número 4 como divisor. Ao efetuarmos a divisão de cada caractere da mensagem cifrada por 4 (da mesma forma como fizemos na Figura 4), considerando os seis primeiros caracteres que correspondem à divisão por 4 que possuem resto 1, obtemos 1, 5, 9, 13, 17, 21, ou seja, HCTAAE, o que parece não ter sentido.

De maneira análoga, procederemos com a divisão por 5. Ao repetirmos o mesmo processo realizado na Figura 5 e, considerando os seis primeiros caracteres que possuem resto 1 na divisão por 5, obtemos 1, 6, 11, 16, 21, 26, que corresponde a sequência de letras HOJEED. Assim, acabamos de obter uma palavra do texto original. Mas para nos certificarmos de que isso não é uma coincidência e que o número de lados da base do polígono regular relativo ao prisma é de fato 5, agruparemos as letras correspondentes aos restos de cada c na divisão por 5, conforme ilustra a Figura 6.

Figura 6 - Restos obtidos ao realizar a divisão euclidiana $c = qb + r; 0 \leq r < b$, em cada caractere presente no texto cifrado. Considere c o caractere respeitando-se a ordem em que aparece na mensagem cifrada (ver Figura 4), r é o resto e q é o quociente na divisão de c por 5.

resto / quociente	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 0$
$q = 0$	H: $1 = 0 * 5 + 1$	A: $2 = 0 * 5 + 2$	I: $3 = 0 * 5 + 3$	A: $4 = 0 * 5 + 4$	
$q = 1$					C: $5 = 1 * 5 + 0$

resto / quociente	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 0$
$q = 1$	O: $6 = 1 * 5 + 1$	D: $7 = 1 * 5 + 2$	D: $8 = 1 * 5 + 3$	T: $9 = 1 * 5 + 4$	
$q = 2$					A: $10 = 2 * 5 + 0$

resto / quociente	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 0$
$q = 2$	J: $11 = 2 * 5 + 1$	E: $12 = 2 * 5 + 2$	A: $13 = 2 * 5 + 3$	E: $14 = 2 * 5 + 4$	
$q = 3$					S: $15 = 3 * 5 + 0$

resto / quociente	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 0$
$q = 3$	E: $16 = 3 * 5 + 1$	A: $17 = 3 * 5 + 2$	D: $18 = 3 * 5 + 3$	M: $19 = 3 * 5 + 4$	
$q = 4$					S: $20 = 4 * 5 + 0$

resto / quociente	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 0$
$q = 4$	E: $21 = 4 * 5 + 1$	T: $22 = 4 * 5 + 2$	E: $23 = 4 * 5 + 3$	A: $24 = 4 * 5 + 4$	
$q = 5$					I: $25 = 5 * 5 + 0$

resto / quociente	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 0$
$q = 5$	D: $26 = 5 * 5 + 1$	I: $27 = 5 * 5 + 2$	S: $28 = 5 * 5 + 3$	T: $29 = 5 * 5 + 4$	
$q = 6$					M: $30 = 6 * 5 + 0$

resto / quociente	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 0$
$q = 6$	I: $31 = 6 * 5 + 1$	V: $32 = 6 * 5 + 2$	M: $33 = 6 * 5 + 3$	I: $34 = 6 * 5 + 4$	

Fonte: elaborado pelos autores (2025).

Observe que ao juntarmos todas as letras na sequência em que os restos a partir de 1, obtemos a mensagem decifrada 'HOJEEDIADEATIVIDADESMATEMATICASSIM' que corresponde a mensagem original 'Hoje é dia de atividades matemáticas? Sim!'.

É interessante notar que, se ao realizarmos as divisões, formos agrupando os resultados em células de tabelas cujo número de colunas for igual ao divisor usado, quando usarmos o divisor correto o texto já estará decifrado se lermos as letras coluna por coluna. Uma ilustração disso está presenta na Figura 7.

Figura 7 - Aplicação da divisão euclidiana $c = qb + r; 0 \leq r < b$, em cada caractere presente no texto cifrado agrupando o caractere c que possui resto $r_i, i = 1, 2, 3, 4, 0$.

Restos	*c*	Mensagem decifrada
1	1, 6, 11, 16, 21, 26, 31	HOJEEDI
2	2, 7, 12, 17, 22, 27, 32	ADEATIV
3	3, 8, 13, 18, 23, 28, 33	IDADESM
4	4, 9, 14, 19, 24, 29, 34	ATEMATI
0	5, 10, 15, 20, 25, 30, 35	CASSIM

Fonte: elaborado pelos autores (2025).

Na Figura 7, considere c o caractere respeitando-se a ordem em que aparece na mensagem cifrada (ver Figura 4), r é o resto e q é o quociente na divisão de c por 5.

Essa é uma característica que pode reduzir o trabalho da decifragem, porém não deve ser mencionada aos alunos, deixando-os intuírem esse detalhe. Seguindo essa abordagem, no momento em que os alunos realizarem as atividades propostas é aconselhável que os mesmos realizem cada divisão presente nas tabelas anteriores anotando os restos para que tenham a oportunidade de reconhecer os padrões que surgem.

Após isso, é conveniente anotar em cada teste com um determinado divisor, apenas os números cujos restos serão o mesmo. Por exemplo, ao dividir os números naturais por 5 como foi feito na Figura 7, já sabemos (e espera-se que os alunos percebam) que os números que deixarão resto 1 são os termos de uma PA (progressão aritmética) de termo inicial 1 e razão 5 dada por $c = 1, 6, 11, 16, 21, 26, 31$. Da mesma forma, os que deixarão resto 2 são os termos de uma PA de termo inicial 2 e razão 5 dada pela sequência $c = 2, 7, 12, 17, 22, 27, 32$. Analogamente, obtemos as sequências para os demais restos associando-as a uma PA.

Isso se justifica justamente pelo caráter de repetição periódica da posição de letras consecutivas do texto original no texto cifrado. Se uma letra qualquer tem a posição x_1 no texto original e posição a_1 no texto cifrado e o citale utilizado para cifragem tem r lados em sua base, a próxima letra do texto original x_2 estará r posições à frente de x_1 no texto cifrado, enquanto x_3 estará r posições à frente de x_2, ou seja, se chamarmos de $P(x)$ a posição no texto cifrado de um caractere de posição genérica x no texto original, teremos as equações descritas na Figura 8.

Figura 8 - Equações obtidas a partir da posição P(x) no texto cifrado de um caractere de posição genérica x no texto original sendo equivalentes a uma progressão aritmética.

$$\begin{array}{ccc} P(x_1) & = & a_1 \\ P(x_2) = P(x_1) + r & = & a_1 + r \\ P(x_3) = P(x_2) + r & = & a_1 + 2r \\ \vdots & \vdots & \vdots \\ P(x_n) = P(x_{n-1}) + r & = & a_1 + (n-1)r \end{array}$$

Fonte: elaborado pelos autores (2025).

4.1.2 Atividade 2: Representar mensagens como vetores numéricos e usar multiplicação de matrizes e matriz inversa para cifrar e decifrar mensagens.

Nesta atividade trabalhamos os conteúdos de matrizes, operações com matrizes, matriz inversa e conversão de dados alfabéticos para dados numéricos. A atividade consistiu em cada grupo escolher uma frase, converter as letras em números através de uma tabela básica de associação alfanumérica e cifrar uma mensagem, multiplicando por uma matriz invertível.

Para a escolha da matriz invertível, algumas matrizes foram fornecidas pelo professor e cada grupo escolheu uma para usar como chave. Em seguida, as mensagens foram trocadas entre os grupos e cada grupo que recebia a mensagem de outro recebia também a chave (matriz) utilizada para cifrar, devendo, portanto, obter a inversa da chave, realizar a multiplicação conveniente e converter novamente os números obtidos em texto.

Utilizamos também a calculadora de matrizes online disponível em (*Matrix Calculator*, 2023), para realizarmos as multiplicações entre matrizes e também a inversão de matriz devido ao pouco tempo para a realização da atividade.

Como ilustração do método, vamos cifrar e decifrar uma mensagem conforme apresentado na Figura 9.

Figura 9 - Descrição do método de cifragem e decifragem por meio de multiplicação de matrizes.

1º) Escolher uma mensagem para ser cifrada: em nosso caso escolhemos 'BOM DIA';

2º) Criar uma tabela e numerar as letras do alfabeto;

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**-**	
15	16	17	18	19	20	21	22	23	24	25	26	27	

3º) Escrever os números correspondentes às letras da mensagem a ser cifrada (representamos os espaços pelo traço que corresponde ao número 27 da tabela do 2º passo);

B	O	M	-	D	I	A
2	15	13	27	4	9	1

4º) Criar a matriz chave que seja invertível (como os alunos deverão inverter a 'Matriz Chave', é interessante que a ordem seja 2, minimizando assim, a dificuldade dos alunos);

$$\text{Matriz Chave} = \begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix}$$

5º) Determinar a matriz que represente a mensagem que será cifrada (é importante atentar-se ao tamanho dessa matriz ao escolher o número de linhas e de colunas, pois esta matriz será multiplicada pela matriz chave);

$\text{Matriz Mensagem} = \begin{bmatrix} 2 & 15 \\ 13 & 27 \\ 4 & 9 \\ 1 & 27 \end{bmatrix}$ Obs: observe que seguimos a sequência dos números preenchendo as linhas. Como a mensagem terminou antes de preenchermos todos os elementos da última linha, inserimos no elemento a_{42} o número 27, que corresponde a um espaço.
6º) Para cifrar a mensagem 'BOM DIA' basta multiplicar a 'Matriz Mensagem' pela 'Matriz Chave'; $\begin{bmatrix} 2 & 15 \\ 13 & 27 \\ 4 & 9 \\ 1 & 27 \end{bmatrix} \cdot \begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 36 & 89 \\ 93 & 226 \\ 30 & 73 \\ 57 & 142 \end{bmatrix} = \text{Mensagem Cifrada}$
7º) Para decifrar a mensagem por meio da matriz 'Mensagem Cifrada', basta multiplicar a matriz 'Mensagem Cifrada' pela inversa da 'Matriz Chave'; $\begin{bmatrix} 36 & 89 \\ 93 & 226 \\ 30 & 73 \\ 57 & 142 \end{bmatrix} \cdot \begin{bmatrix} 5 & -7 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 15 \\ 13 & 27 \\ 4 & 9 \\ 1 & 27 \end{bmatrix} = \text{Mensagem "BOM DIA"}$

Fonte: elaborado pelos autores (2025).

4.1.3 Atividade 3: cifragem por transposição

Nesta atividade exploramos o princípio fundamental da contagem e alguns tópicos de análise combinatória. A cifragem por citale e alguns outros métodos específicos de cifragem pertencem a um grupo geral de cifras chamadas cifras de transposição. É caracterizado por uma troca da posição dos caracteres do texto original no texto cifrado, em que cada letra de uma frase por exemplo, estará em uma posição diferente no texto cifrado daquela em que se encontrava no texto original.

Nas cifras de transposição temos como resultado um anagrama (termo normalmente usado para se referir às palavras compostas pelas mesmas letras, porém, em ordens diferentes) do texto original. Por exemplo, a palavra 'bola' é um anagrama da palavra 'loba' e a palavra 'socar' é um anagrama da palavra 'rocas'. Qualquer combinação nova das letras originais é um anagrama sem que seja necessário que a nova combinação tenha algum sentido textual, assim 'ablo' e 'ocsar' também são anagramas de 'loba' e 'rocas' respectivamente. É possível cifrar qualquer texto apenas gerando um anagrama qualquer do mesmo, e isso possibilita um número de diferentes cifragens que aumenta rapidamente conforme se aumenta o número de caracteres do texto (Ver Figura 10).

Figura 10 - Diferentes cifragens que aumentam conforme o número de caracteres é aumentado.

Número de letras da palavra	Número de anagramas possíveis	anagramas possíveis
2 letras	2	• ai/ia • ou/uo
3 letras	6	• foi/fio/ofi/oif/ifo/iof • olá/oal/loa/lao/alo/aol
4 letras	24	• beco/beoc/boce/boec/bcoe/bceo/ebco /eboc/ecbo/ecob/eocb/eobc/ • cebo/ceob/cbeo/cboe/cobe/coeb/oceb /ocbe/oecb/oebc/obce/obec

Fonte: elaborado pelos autores (2025).

A cada letra que adicionamos à palavra, o número de anagramas possíveis corresponde ao número de anagramas da quantidade anterior de letras vezes o número de letras atual. Isso se deve ao fato de que o número de anagramas é o número de permutações simples possíveis para uma dada quantidade de letras, logo para uma palavra de n letras temos $n!$ anagramas possíveis.

Observe, porém, que entre todos os anagramas possíveis podemos ter alguns repetidos caso hajam letras repetidas na palavra, o que certamente acontecerá caso queiramos formar anagramas de uma frase ou um texto, observe um exemplo com a palavra uau, onde enumeramos cada letra com um índice para facilitar a distinção entre os dois 'us' presentes na palavra, resultando em u1a2u3/u1u3a2/a2u3u1/a2u1u3/u3a2u1/u3u1a2.

Como era de se esperar, obtemos 6 anagramas para uma palavra que possui 3 letras, porém, com apenas 3 anagramas distintos. Para uma palavra, frase ou texto qualquer, temos um número específico de possíveis anagramas que corresponde ao número de possíveis cifragens por transposição. Entretanto é evidente que a elaboração de dois textos cifrados que sejam iguais, a partir de um mesmo texto original não tem sentido lógico, pois devemos distinguir o número de cifras de transposição possível do número de cifras de transposição que resultam em textos distintos.

Apesar do número de cifragens por transposição ser altíssimo para textos que possuem um número alto de caracteres, na prática, a cifragem não pode ser feita de modo aleatório, pois isso impossibilitaria a decifragem posterior. Dessa forma, devemos cifrar um texto por transposição através de algum método bem definido de cifragem, como o citale. Nesses casos, a cifra definida para transpor os caracteres pode ser representada matematicamente por uma função bijetiva sobre o conjunto das posições do caractere no texto, enquanto que o processo de decifragem é a correspondente função inversa. A seguir apresentamos três cifras simples de transposição.

1ª) Cifra de colunas: Os caracteres do texto a ser cifrado são escritos em colunas formando uma grade com um número de linhas pré definido. Quando o número de linhas é atingido em uma coluna, a escrita continua na coluna seguinte e, ao final, caso a última coluna não seja inteiramente preenchida, é possível inserir caracteres aleatórios para completar a grade. A mensagem cifrada é formada pelos caracteres na ordem em que ficam dispostos nas linhas da grade, conforme a aplicação ilustrativa a seguir. Considere a mensagem original 'Não revele essa mensagem' inserindo-a em uma grade

contendo 4 linhas. Para decifrar a mensagem basta que o destinatário conheça o número fixo de linhas utilizadas na grade, dividindo o número de caracteres da mensagem por esse número, obtendo assim, o número de colunas nas quais ele deve distribuir os caracteres da mensagem cifrada escrevendo-os linha por linha, e lê-los coluna por coluna. Essa cifra é muito semelhante à do citale, porém sem a necessidade de um objeto físico para realizar a cifragem conforme ilustrado na Figura 11. Especificamente, se fizermos um processo análogo à cifra das colunas, porém distribuindo os caracteres em linhas numa grade com o número de colunas fixo obteremos exatamente uma cifra por citale.

Figura 11 - Cifragem e decifragem por colunas da mensagem 'Não revele essa mensagem'.

Cifragem

Tabela com 4 linhas sendo as letras da mensagem distribuídas verticalmente em colunas (os 3 espaços que sobraram foram preenchidos com as letras aleatórias R, T, I).

N	E	E	A	S	M
A	V	E	M	A	R
O	E	S	E	G	T
R	L	S	N	E	I

Mensagem cifrada: N E E A S M A V E M A R O E S E G T R L S N E I

Decifragem

$$\frac{n^o \text{ de caracteres mensagem cifrada}}{n^o \text{ de linhas utilizadas}} = n^o \text{ de colunas que serão distribuídos os caracteres da mensagem cifrada}$$

$$24\ caracteres \div 4\ linhas = 6 \text{ colunas}$$

Distribua os caracteres da mensagem cifrada horizontalmente (nas linhas) e leia verticalmente (colunas)

N	E	E	A	S	M
A	V	E	M	A	R
O	E	S	E	G	T
R	L	S	N	E	I

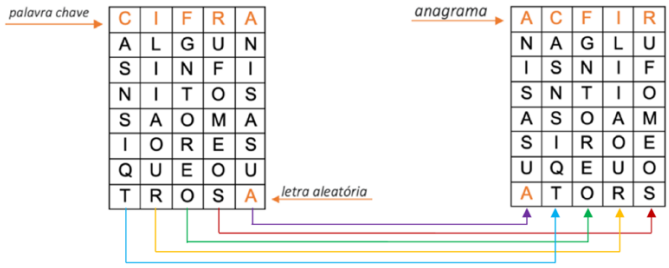
Fonte: elaborado pelos autores (2025).

2ª) Cifra por transposição de colunas: uma palavra chave é escrita na primeira linha de uma grade e, em seguida, a mensagem a ser cifrada é escrita abaixo, linha por linha com um total de colunas igual ao número de letras da palavra chave. A mensagem cifrada é obtida através da transcrição das colunas por ordem alfabética das letras da palavra chave. A Figura 12, ilustra como cifrar e decifrar a mensagem 'alguns infinitos são maiores que outros' usando a palavra-chave 'cifra'.

Figura 12 - Cifragem e decifragem por transposição de colunas da mensagem ‘alguns infinitos são maiores que outros’ com palavra-chave ‘cifra’.

Cifragem

Criar uma tabela com 5 colunas correspondendo ao no de caracteres da palavra-chave ‘CIFRA’. Escrevemos a mensagem em linhas, distribuindo os caracteres em colunas, respeitando o número de colunas definido pela chave. Rearranjamos as colunas de acordo com a ordem alfabética da chave ‘CIFRA’ criando o anagrama ‘ACFIR’. A mensagem cifrada é formada lendo os caracteres coluna por coluna, seguindo a nova ordem.



Mensagem cifrada obtida pelas colunas:

N	I	S	A	S	U	A	A	S	N	S	I	Q	T	G	N	T	O	R	E	O	L	I	I	A	O	U	R	U	F	O	M	E			

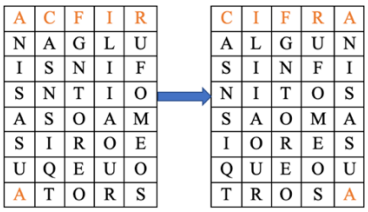
Decifragem

O destinatário deve conhecer a palavra chave utilizada. Daí fazendo,

$$\frac{n^o\ de\ caracteres\ mensagem\ cifrada}{n^o\ de\ caracteres\ da\ \ palavra\ chave} = n^o\ de\ linhas\ que\ serão\ distribuídos\ os\ caracteres\ da\ mensagem\ cifrada$$

$$35\ caracteres\ mensagem\ cifrada \div\ 5\ caracteres\ palavra\ chave = 7\ linhas$$

Levando-se em conta que temos 5 caracteres para a palavra-chave ‘CIFRA’ então nossa tabela de decifragem terá 7 linhas e 5 colunas (sem contar com a linha da palavra-chave). Distribuímos a mensagem cifrada nas colunas da tabela composta pelo anagrama ‘ACFIR’ e depois reordenamos as colunas obtendo ‘CIFRA’. Daí, é só ler a mensagem linha por linha.



Fonte: elaborado pelos autores (2025).

3ª) Cifra das espirais: este é um conjunto de cifras que são na verdade variações de uma mesma ideia escrevendo-se os caracteres da mensagem a ser cifrada em uma grade retangular como nas cifras anteriores. Com isso, obtemos o texto cifrado transcrevendo os caracteres na ordem em que aparecem

segundo uma 'espiral retangular' construída sobre a grade. Na Figura 13, ilustramos como cifrar e decifrar a mensagem 'cifras das espirais' utilizando o método.

Figura 13 - Cifragem e decifragem por cifra das espirais da mensagem 'Cifras das espirais'.

Cifragem
Escrevendo a mensagem 'CIFRAS DAS ESPIRAIS' em uma grade/retangular (escolhemos o número de linhas e colunas baseado no tamanho da mensagem). Preenchemos as linhas com os caracteres da mensagem da esquerda para a direita e de cima para baixo. Se sobrar espaços em branco, usamos caracteres aleatórios. C I F R A S D A S E S P I R A I S V A leitura da mensagem cifrada segue um percurso em espiral, começando do canto superior direito e se movendo no sentido horário, obtendo a seguinte mensagem cifrada: S A R F I C D I R A I S V P S E S A *Existem inúmeras variações dessa ideia que podem ser obtidas pelas combinações das diferentes opções da distribuição dos caracteres na grade com as diferentes opções de construção da espiral:* • *a mensagem pode ser escrita na grade linha por linha ou coluna por coluna.* • *a espiral pode ser construída em sentido horário ou anti-horário.* • *a espiral pode ser construída das bordas para o centro ou do centro para as bordas.* • *a espiral pode iniciar (quando construída da borda para o centro) ou terminar (quando construída do centro para a borda) em qualquer um dos quatro vértices da grade.*
Decifragem
O destinatário precisa sabe o tamanho da grade/matriz (em nosso caso 3×6) e também qual é o percurso da espiral. Em seguida, preencher a matriz com os caracteres da mensagem cifrada seguindo o caminho da espiral. Feito isso, basta ler a matriz (linha por linha) para recuperar a mensagem original.

Fonte: elaborado pelos autores (2025).

Outras técnicas de cifragem, como por exemplo por substituição (cifra de César, cifra de deslocamento por palavra-chave, cifra do chiqueiro, entre outras) podem ser encontradas em (Rodrigues, 2024). Nosso objetivo aqui, consiste apenas em ilustrar formas de interagir a matemática ensinada nas escolas com atividades motivadoras e criativas.

5 REFLEXÕES FINAIS

Concluímos que, os conteúdos matemáticos trabalhados, bem como as atividades práticas elaboradas e implementadas em turmas do Ensino Fundamental II e Ensino Médio ofereceram um outro olhar em relação à didática empregada em sala de aula. A utilização de técnicas criptográficas como o citale, a multiplicação de matrizes, a inversão matricial e as cifras por transposição, permitiu aos estudantes explorar conceitos matemáticos de forma prática, desafiadora e intelectualmente estimulante. Ao lidar com problemas reais de codificação e decodificação, os alunos desenvolveram habilidades de raciocínio lógico, análise e tomada de decisão, aproximando o estudo da Matemática a situações reais.

Esse potencial se amplia quando analisado à luz da Aprendizagem Significativa. As atividades de criptografia favoreceram a articulação entre novos conteúdos e conhecimentos prévios, criando espaços nos quais os alunos puderam reorganizar suas estruturas cognitivas e atribuir sentido aos procedimentos matemáticos utilizados. A contextualização, elemento central da teoria de Ausubel, mostrou-se decisiva para que os estudantes percebessem propósitos concretos para aprender aritmética modular, progressões aritméticas ou operações matriciais, reduzindo a fragmentação do ensino e promovendo aprendizagens mais duradouras.

Paralelamente, observa-se que as propostas desenvolvidas dialogam diretamente com princípios da Aprendizagem Baseada em Projetos (ABP). As atividades de criptografia configuram desafios abertos, que exigem investigação, colaboração e a elaboração de estratégias próprias para resolver problemas. Assim como defendem autores como Dewey, Vygotsky e Thomas, aprender por meio de projetos aproxima os estudantes de situações reais, sustenta o engajamento e fortalece a autonomia intelectual. No trabalho apresentado, a criptografia funcionou como eixo gerador capaz de integrar conteúdos matemáticos, promover propósito claro de aprendizagem e favorecer a construção ativa do conhecimento, que se tratam, de elementos centrais tanto da ABP quanto da aprendizagem significativa. Dessa forma, evidencia-se que a abordagem não apenas motiva, mas cria condições efetivas para que os alunos atribuam significado ao que aprendem, consolidando conceitos de maneira integrada e contextualizada.

No contexto pedagógico, refletir sobre essas experiências permite reconhecer o valor de atividades que conectam álgebra, teoria dos números e representações matriciais à resolução de desafios práticos. Ao lidar com códigos, matrizes e transformações de mensagens, os estudantes não apenas compreendem estruturas lógicas, mas também percebem a utilidade da Matemática para resolver problemas contemporâneos, como segurança da informação e comunicação digital e tratamento de dados, ampliando a relevância social do conhecimento escolar.

Do ponto de vista metodológico, este estudo caracteriza-se como uma pesquisa qualitativa de natureza aplicada, uma vez que analisa práticas educativas reais e busca propor intervenções que contribuam para o ensino da Matemática. Tal abordagem é coerente com referenciais metodológicos da Educação Matemática, conforme discutido no trabalho de Melo (2014), que enfatizam a observação interpretativa e a análise descritiva das experiências de sala de aula como meios adequados para

compreender processos de aprendizagem. Assim, a pesquisa não se limita à descrição das atividades, mas procura interpretar como elas favorecem engajamento, construção de significados e desenvolvimento conceitual. Detalhes específicos sobre este trabalho nesse sentido, podem ser encontrados em Rodrigues (2024).

Em síntese, as atividades de criptografia mostraram-se um recurso potente para tornar o ensino de Matemática mais contextualizado, interdisciplinar e motivador. Ao integrar ABP, Aprendizagem Significativa e desafios criptográficos, este estudo evidencia um caminho pedagógico que combina rigor conceitual, criatividade e relevância, contribuindo para aproximar os estudantes de práticas matemáticas mais vivas, significativas e conectadas ao mundo contemporâneo.

REFERÊNCIAS

AUSUBEL, D.P. Psicologia Educacional: Uma Visão Cognitiva. Nova York, NY: Holt, Rinehart e Winston, 1968.

BALL, D. L. The mathematical understandings that prospective teachers bring to teacher education. Elementary School Journal, v. 90, n. 4, p. 449–466, 1990.

BOALER, Jo. Mathematical mindsets: Unleashing students' potential through creative math, inspiring messages and innovative teaching. San Francisco: Jossey-Bass, 2016.

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. Brasília: MEC, 2017.

CASTELLAR, S. A construção do pensamento algébrico na escola: desafios e possibilidades. Belo Horizonte: Autêntica Editora, 2014.

D'AMBRÓSIO, U. Educação matemática: da teoria à prática. Campinas: Papirus, 1996.

DEWEY, J. Democracia e Educação: introdução à filosofia da educação. 4.ed. John Dewey; tradução de Godofredo Rangel e Anísio Teixeira. 4. ed. São Paulo: Ed. Nacional, 1979.

FIORENTINI, D. e LORENZATO, S. Investigação em educação matemática: percursos teóricos e metodológicos. Campinas: Autores Associados, 2006.

FREIRE, P. Educação e mudança. Rio de Janeiro: Paz e Terra, 1973.

MATRIX CALCULATOR. Disponível em: https://matrixcalc.org/pt/. Acesso em: 25/10/2023.

MELO, C. D. L. (2014). Criptografia no Ensino Médio: uma Proposta para o Ensino de Matrizes. Dissertação de Mestrado, Universidade Estadual de Campinas, Campinas.

OLIVEIRA, M.K. Vygotsky: aprendizagem e desenvolvimento de um processo sócio-histórico. São Paulo: Cipione, 2016.

PONTES, E. A. S., SILVA, B. H. M. S., & OLIVEIRA, E. G. (2022). Criptografia em Funções Polinomiais: Um Processo de Ensino e Aprendizagem de Matemática na Educação Básica. The Journal of Engineering and Exact Sciences, 8(6), 14609-01e.

RODRIGUES, I. R. (2024). Uso de Ferramentas de Criptografia no Ensino de Matemática para os Ensinos Fundamental II e Médio: Proposta de Atividades. Orientador: Raul Abreu de Assis, 2024. 112 f.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional). Faculdade de Ciências Exatas e Tecnológicas, Universidade do Estado de Mato Grosso, Sinop, 2024. Disponível em: https://profmat-sbm.org.br/dissertacoes/?aluno=isac&titulo=&polo= Acesso em: 27/11/2025.

SILVA, M. V., EVANGELISTA, D. H. R., & EVANGELISTA, C. J. (2022). Tecnologias digitais aliadas ao ensino de Criptografia. The Journal of Engineering and Exact Sciences, 8(5), 14313-01e.

THOMAS, J.W. Uma revisão da pesquisa sobre aprendizagem baseada em projetos. San Rafael, CA: Fundação Autodesk, 2000.

VIDAL, S. C., CAPRI, M. R., & ROMÃO, E. C. (2022). Cryptography as an Educational Tool in Counting Techniques for High School. International Journal for Innovation Education and Research, 10(5), 76-88.

VYGOTSKY, L.S. Mente na Sociedade: O Desenvolvimento de Processos Psicológicos Superiores. Cambridge, MA: Harvard University Press, 1978.

Recebido em: 28 de fevereiro de 2025.
Aprovado em: 23 de novembro de 2025.
DOI: https://doi.org/10.30681/reps.v16i3.13527

[i] Isac Rosa Rodrigues. Graduado em Ciências Naturais e Matemática - Física, Licenciatura pela Universidade Federal do Mato Grosso UFMT - Campus Sinop (2019); Especialista em Ciências Exatas pela Faculdade Focus (2023); Mestre em Matemática pelo Mestrado Profissional em Matemática em rede nacional (PROFMAT). Atuou como monitor nas disciplinas de Geometria, Cálculo I e Cálculo II durante a graduação; atuou como professor na Faculdade de Tecnologia de Sinop (FASTECH) na disciplina de Física I; atua como professor contratado na Universidade Federal de Mato Grosso (UFMT), campus Várzea Grande como professor da área de Matemática.
Curriculum Lattes: http://lattes.cnpq.br/5651702834620067
ORCID: https://orcid.org/0009-0002-9471-8058
E-mail: rodrigues.isac@unemat.br

[ii] Luciana Assis. Possui doutorado em "Sistemas Complexos para as Ciências da Vida" pela Universidade de Estudos de Torino - Itália (UNITO) com ênfase em Matemática Aplicada. Atualmente é professora lotada na Faculdade de Ciências Exatas e Tecnológicas (FACET) da Universidade do Estado de Mato Grosso (UNEMAT). Tem experiência na área de Matemática com ênfase em Modelagem Matemática para o Ensino e Álgebra.
Curriculum Lattes: http://lattes.cnpq.br/4987775675315381
ORCID: https://orcid.org/0000-0002-7247-0429
E-mail: luciana.assis@unemat.br

[iii] Raul Abreu de Assis. Possui Doutorado em Matemática Aplicada pela Universidade Estadual de Campinas e Pós-doutorado pela Universidade de Estudos de Torino - Itália (UNITO). Atualmente é professor lotado na Faculdade de Ciências Exatas e Tecnológicas (FACET) da Universidade do Estado de Mato Grosso. Tem experiência na área de Matemática Aplicada com ênfase em biomatemática, atuando principalmente nos seguintes temas: dinâmicas evolutivas, modelos de evolução e equações diferenciais.
Curriculum Lattes: http://lattes.cnpq.br/7738144067749993
ORCID: https://orcid.org/0000-0002-0473-9211
E-mail: raulassis@unemat.br