

Explorando Funções Afins e Criptografia: Reflexões e Resultados de uma Oficina Pedagógica

Fernanda Vital de Paula¹

Ariane Andressa Noronha de Sousa Miranda²

Resumo: A criptografia, essencial à segurança digital, é um tema instigante para relacionar funções afins com situações reais e despertar o interesse dos alunos pela matemática. Este relato de experiência analisa uma oficina aplicada no 9º ano do Ensino Fundamental e no 3º ano do Ensino Médio, que utilizou a criptografia para ensinar funções afins de maneira contextualizada. Por meio de questionários aplicados aos estudantes e das observações da professora responsável pela oficina, avaliou-se a eficácia da proposta. Os resultados indicaram que a abordagem contextualizada, ao articular o conteúdo de função afim com a história e o funcionamento da criptografia, facilitou a compreensão do conteúdo, especialmente no Ensino Fundamental, onde se observou maior engajamento. Já no Ensino Médio, sugere-se a incorporação de tecnologias como estratégia para ampliar a motivação. Conclui-se que a criptografia, por sua presença no cotidiano, é um tema promissor para tornar o ensino da matemática mais dinâmico e significativo.

Palavras-chave: Criptografia. Ensino Contextualizado. Funções Afins.

Exploring Affine Functions and Cryptography: Reflections and Outcomes of a Pedagogical Workshop

Abstract: Cryptography, essential to digital security, is a compelling topic for connecting affine functions with real-life situations and sparking students' interest in mathematics. This experience report analyzes a workshop conducted with 9th-grade middle school and 3rd-year high school students, which used cryptography to teach affine functions in a contextualized way. Through questionnaires administered to students and observations made by the teacher responsible for the workshop, the effectiveness of the proposal was evaluated. The results indicated that the contextualized approach, linking the concept of affine function to the history and operation of cryptography, facilitated content comprehension, especially in middle school, where greater engagement was observed. In high school, however, the incorporation of technology is suggested as a strategy to enhance motivation. It is concluded that, due to its presence in everyday life, cryptography is a promising theme for making mathematics teaching more dynamic and meaningful.

Keywords: Cryptography. Contextualized Teaching. Affine Functions.

Explorando Funciones Afines y Criptografía: Reflexiones y Resultados de un Taller Pedagógico

Resumen: La criptografía, esencial para la seguridad digital, constituye un tema estimulante para relacionar funciones afines con situaciones reales y despertar el interés del alumnado por las matemáticas. Este informe de experiencia analiza un taller aplicado en el 9.º grado de la Educación Básica y en el 3.º año de la Educación Media, que utilizó la criptografía para enseñar funciones afines de forma contextualizada. A través de cuestionarios aplicados a los estudiantes y de observaciones realizadas por la docente responsable del taller, se evaluó la eficacia de la propuesta. Los resultados indicaron que el enfoque contextualizado, al articular el contenido de funciones afines con la historia y el funcionamiento de la criptografía, facilitó la comprensión del contenido, especialmente en la Educación Básica, donde se observó mayor participación. En la Educación Media, se sugiere la incorporación de tecnologías como estrategia para aumentar la motivación. Se concluye que la

¹ Doutora em Estatística. Universidade Federal do Norte do Tocantins. Araguaína, TO, Brasil. E-mail: fernanda.paula@ufnt.edu.br - Orcid: <https://orcid.org/0000-0002-7936-8937>.

² Licenciada em Matemática. Colégio Estadual José Luiz Siqueira. Wanderlândia, TO, Brasil. E-mail: ariane.andressa@mail.uft.edu.br - Orcid: <https://orcid.org/0000-0003-2322-1554>.

criptografia, por su presencia en la vida cotidiana, es un tema prometedor para hacer que la enseñanza de las matemáticas sea más dinámica y significativa.

Palabras clave: Criptografía. Enseñanza contextualizada. Funciones afines.

1 Introdução

Ao buscar conexões entre o conhecimento matemático e situações reais, o educador fortalece o raciocínio dos alunos, promovendo competências como resolução de problemas, criatividade e autonomia, essenciais para o desenvolvimento do pensamento lógico. Nessa perspectiva, a criptografia pode ser utilizada para atribuir significado aos conteúdos matemáticos, por meio de situações que refletem a realidade dos alunos.

No cotidiano, todos os indivíduos possuem informações que precisam ser mantidas em sigilo, como conversas em aplicativos de mensagens, registros de transações bancárias, *e-mail*, informações militares, dados de clientes, entre outros. Essa necessidade deu origem à criptografia, desenvolvida inicialmente em períodos de guerra para garantir a segurança na troca de informações. Derivada do grego *kriptos* (escondido) e *grapho* (escrita), a criptografia é um mecanismo de codificação de mensagens cujo objetivo é garantir que apenas seu destinatário legítimo, utilizando uma chave específica, possa decifrá-la. Nesse sentido, “o objetivo dos sistemas criptográficos não é esconder a existência de uma mensagem, mas evitar que uma pessoa desautorizada compreenda o seu significado, mesmo que tenha acesso às informações cifradas” (Menezes, 2013, p. 16).

Diante disso, Miranda e Paula (2021) propuseram uma oficina pedagógica com o objetivo de empregar a função afim na codificação e decodificação de mensagens, permitindo que alunos da Educação Básica compreendam o funcionamento e a importância da criptografia de maneira acessível. Embora a criptografia, na prática, utilize técnicas e conceitos mais complexos, a oficina buscou simplificar o tema. As autoras destacam que a escolha da oficina como ferramenta de ensino visa contribuir para a desmistificação da matemática, muitas vezes vista como uma matéria de difícil assimilação, e explorar uma abordagem de ensino e aprendizagem que se diferencia do modelo tradicional.

Com o intuito de avaliar a oficina proposta pelas autoras e explorar seu potencial, este artigo apresenta os resultados obtidos a partir de sua aplicação em duas turmas: uma do 9º ano do Ensino Fundamental e outra do 3º ano do Ensino Médio. A avaliação da oficina foi realizada por meio da aplicação de questionários aos alunos participantes e do relato pessoal da professora que conduziu a atividade. Os resultados obtidos serão apresentados e analisados ao longo deste trabalho.

2 Referencial Teórico

Menezes (2013, p. 15) aponta que a ameaça de interceptação de mensagens por espões não apenas incentivou o desenvolvimento de métodos para torná-las ininteligíveis, mas também deu origem a técnicas para ocultá-las. A criptografia opera como um sistema de algoritmos que embaralha o conteúdo das mensagens, passando pelas fases de codificação e decodificação. Codificar envolve converter os elementos de uma mensagem em símbolos secretos, um processo também conhecido como encriptação ou ciframento, que transforma a informação por meio de um algoritmo. Posteriormente, o destinatário recebe a mensagem e a decodifica. Sobre as origens da criptografia, Galdino (2014, p. 5) destaca uma das primeiras referências datada de 480 a.C., em que Heródoto escreveu sobre os conflitos entre Grécia e Pérsia.

Dando continuidade ao panorama histórico, Galdino (2014, p. 50) também menciona que o imperador romano Júlio César (100 a.C. - 44 a.C.) usava um sistema criptográfico que consistia em uma técnica de transposição de letras que eram substituídas por letras localizadas exatamente três posições adiante no alfabeto. Assim, codificar uma mensagem usando a cifra de César consiste em deslocar cada letra do alfabeto original de acordo com um número natural k menor que 26, que indica o número de posições de deslocamento. Ao codificar a palavra AMOR, por exemplo, com $k = 3$, obtém-se DPRU. Observe que $A (1) \rightarrow D (1+3)$; $M (13) \rightarrow P (13+3)$; $O (15) \rightarrow R (15+3)$ e $R (18) \rightarrow U (18+3)$.

Com o avanço da matemática e da tecnologia, vários métodos criptográficos foram desenvolvidos para garantir a segurança em atividades que exigem sigilo. Nesse contexto, Reis (1989, p. 8) menciona que, com o surgimento do computador, novas aplicações para a criptografia foram criadas, como a transferência automática de fundos e a proteção de dados em arquivos. Assim, diversas empresas passaram a investir em ferramentas tecnológicas de segurança baseadas em criptografia. Um dos métodos mais utilizados por essas empresas é a criptografia Rivest-Shamir-Adleman (RSA). O método RSA utiliza números primos para criar uma chave de codificação. Devido à grande magnitude dos números envolvidos, mesmo aqueles que conhecem a chave pública não têm acesso aos números necessários para decodificação, o que garante a segurança do processo.

Na Educação Básica, a criptografia pode ser incorporada em diversas atividades. É possível introduzir o tema no ensino de conteúdos da Base Nacional Comum Curricular (BNCC), como matrizes e funções, utilizando métodos criptográficos mais simples, anteriores ao método RSA, como a cifra de Hill. A cifra de Hill, criada em 1929 por Lester Hill, é um

algoritmo de substituição baseado na álgebra linear. Para torná-la acessível aos alunos do Ensino Fundamental, a cifra de Hill pode ser adaptada mediante a substituição do uso de matrizes por funções inversíveis, facilitando o entendimento e a aplicação dos conceitos criptográficos no ambiente escolar.

Além dos objetos de conhecimento previstos pela BNCC possibilitarem a inserção da criptografia na Educação Básica, o documento também abre espaço para sua introdução em alguns trechos específicos. Um deles, referente ao Ensino Fundamental, afirma:

As competências que estão diretamente associadas a representar pressupõem a elaboração de registros para evocar um objeto matemático. Apesar de essa ação não ser exclusiva da Matemática, uma vez que todas as áreas têm seus processos de representação, em especial nessa área é possível verificar de forma inequívoca a importância das representações para a compreensão de fatos, ideias e conceitos, uma vez que o acesso aos objetos matemáticos se dá por meio delas. Nesse sentido, na Matemática, o uso dos registros de representação e das diferentes linguagens é, muitas vezes, necessário para a compreensão, a resolução e a comunicação de resultados de uma atividade. Por esse motivo, espera-se que os estudantes conheçam diversos registros de representação e possam mobilizá-los para modelar situações diversas por meio da linguagem específica da matemática – verificando que os recursos dessa linguagem são mais apropriados e seguros na busca de soluções e respostas – e, ao mesmo tempo, promover o desenvolvimento de seu próprio raciocínio (Brasil, 2018, p. 529).

Diante disso, Rodrigues e Sá (2019) ilustram a aplicabilidade do conteúdo de matrizes por meio de uma atividade envolvendo criptografia em uma turma do 2º ano do Ensino Médio. De forma semelhante, Olgin e Groenwald (2011) utilizam o conteúdo de funções exponenciais e logarítmicas em uma atividade de criptografia voltada a uma turma do 3º ano do Ensino Médio. Mais recentemente, Kranz e Olgin (2022) aplicaram a cifra de Hill no ensino de matrizes para o 3º ano do Ensino Médio, utilizando planilhas eletrônicas como ferramenta de apoio.

Na mesma linha, Miranda e Paula (2021) propuseram uma oficina pedagógica com o objetivo de utilizar funções afins para codificar e decodificar mensagens, direcionada aos alunos do 9º ano do Ensino Fundamental. A oficina visa conectar a teoria das funções afins à realidade dos alunos, que utilizam cada vez mais aplicativos que empregam métodos criptográficos para garantir segurança e sigilo. Essa abordagem permite que a matemática se torne mais significativa para os alunos e desperte seu interesse pela disciplina.

Conforme as autoras, a escolha da oficina como ferramenta de ensino visou colaborar com a desmistificação da matemática, frequentemente vista como uma disciplina difícil de assimilar, ao explorar uma abordagem de ensino e aprendizagem diferente do tradicional com

um tema capaz de despertar o interesse dos estudantes. Nesse sentido, Almouloud et al. (2021) destacam que

A Criptografia fascina pessoas de todas as gerações e, passou a ser um elemento decisivo do cotidiano das pessoas que possuem e/ou têm acesso a serviços como e-mail, aplicativos de bancos e outros serviços online e necessitam de senhas ou outros códigos para acessar esses ou outros serviços digitais (Almouloud *et al.*, 2021, p. 23).

Reconhecendo a potencialidade da oficina proposta por Miranda e Paula (2021), a atividade foi retomada e desenvolvida neste trabalho com base nas diretrizes originalmente apresentadas.

3 Metodologia

A proposta de desenvolver uma oficina envolvendo funções afins e criptografia, publicada em Miranda e Paula (2021), bem como os resultados compartilhados neste trabalho, foram motivados pelo Programa Residência Pedagógica (PRP). Uma das autoras foi bolsista do PRP de agosto de 2018 a dezembro de 2019, no Colégio Estadual Jorge Amado (CEJA), situado no Setor Noroeste em Araguaína-TO. Como participante do PRP, que oferece uma carga horária superior à do estágio supervisionado, a autora teve a oportunidade de aplicar métodos de ensino alternativos, como oficinas, em vez de seguir exclusivamente abordagens tradicionais.

A oficina foi, portanto, desenvolvida no CEJA, tendo como público-alvo inicial o 9º ano do Ensino Fundamental. No entanto, durante a aplicação em sala de aula, uma das autoras deste artigo expandiu o público para incluir duas turmas: uma do 9º ano do Ensino Fundamental e outra do 3º ano do Ensino Médio. As informações detalhadas sobre essas turmas estão apresentadas no Quadro 1.

Quadro 1: Dados das turmas

Ano	Etapa	Nº de alunos	Tempo de duração
9º	Fundamental	11	1 hora e 40 minutos
3º	Médio	12	1 hora e 40 minutos

Fonte: Autoras (2023)

O objetivo de incluir tanto o Ensino Fundamental quanto o Médio foi explorar a potencialidade da oficina em diferentes níveis de ensino. Para o desenvolvimento da oficina em ambas as turmas, foram executados os três momentos sugeridos e detalhados por Miranda e Paula (2021), a saber:

- 1º Momento: abordagem histórica

Inicialmente, a história da criptografia foi introduzida aos alunos, incluindo detalhes sobre seu uso estratégico em guerras e, principalmente, o funcionamento da cifra de César, a fim de motivar os alunos com os porquês da criação de códigos e sua evolução conforme o desenvolvimento tecnológico. Para buscar a identificação dos estudantes com o assunto, exibiu-se a tela inicial do aplicativo *WhatsApp* e questionou-se se sabiam o significado da palavra “criptografia” e por que ela aparecia na interface do aplicativo. À medida que os alunos respondiam, destacou-se a evolução da criptografia e sua presença no cotidiano. Como parte da atividade, os alunos receberam o desafio de decifrar a mensagem “ocvgocvkec igpkcn”, codificada por meio da substituição de cada letra pela segunda letra seguinte no alfabeto, resultando na mensagem decodificada “matemática genial”. Optou-se por uma transposição simples, semelhante à utilizada por César, para que os estudantes pudessem se ambientar com a ideia de criar e interpretar códigos.

- 2º Momento: revisão das funções afins;

No segundo momento, foram revisados conceitos como domínio, contradomínio e imagem de uma função, bem como as classificações das funções em injetoras, sobrejetoras e bijetoras. Em seguida, foram definidas as funções afins e, como exemplo, foi determinada a inversa da função f , dada algebricamente por $f(x) = 3x + 2$, como $f^{-1}(x) = (x - 2)/3$. Destacou-se também que uma função afim constante, do tipo $g(x) = a$, onde a é uma constante real, não é injetora e, portanto, não admite inversa, sendo inadequada para os propósitos da oficina.

É importante lembrar que, graças ao Programa Residência Pedagógica, uma das autoras deste relato, que à época da oficina era bolsista do Programa, já estava atuando na escola há alguns meses, e o conteúdo de funções afins já havia sido desenvolvido com os alunos. No dia da aplicação da oficina, foi realizada apenas uma revisão com exemplos, essenciais para a etapa seguinte de codificação e decodificação.

- 3º Momento: prática de codificação e decodificação.

Cada turma foi dividida em quatro grupos, e cada grupo elaborou uma mensagem para codificação, utilizando uma tabela de pré-decodificação disponibilizada aos alunos, na qual cada letra correspondia a um número: $A = 1$, $B = 2$, e assim sucessivamente até $Z = 26$. Havia também códigos numéricos para o espaço entre palavras (27), o ponto final (28), a vírgula (29), o ponto de interrogação (30) e o ponto de exclamação (31). Essa tabela permaneceu projetada

durante toda a atividade, assegurando que todos utilizassem o mesmo sistema, essencial para o sucesso da decodificação.

Para que os alunos compreendessem todo o processo, utilizou-se como exemplo a palavra “casa”. As letras foram substituídas pelos números correspondentes e, em seguida, os estudantes criaram uma função afim. Com essa função, cada número foi transformado em um novo valor, substituindo-se o x da função pelo número original de cada letra. Ao final, os alunos determinaram a função inversa e aplicaram-na aos valores codificados para verificar o processo de decodificação.

Por fim, foi orientado que cada grupo escrevesse sua própria mensagem, codificasse e a registrasse em um papel, juntamente com a chave (a função afim criada por eles). Embora a sugestão fosse que escrevessem frases, os alunos optaram por codificar apenas palavras. Após criptografar suas mensagens, elas foram trocadas aleatoriamente entre os grupos para serem decifradas.

Esse processo permitiu que todos os estudantes participassem ativamente da criptografia e da decodificação, além de praticarem cálculos envolvendo funções afins. Também tiveram a oportunidade de definir novas chaves para suas mensagens.

Para a decodificação, os alunos recebiam uma sequência de números e uma chave (função afim). Primeiramente, encontravam a função inversa e, utilizando os números recebidos, calculavam novos valores. Esses valores eram então substituídos por letras, usando a tabela, permitindo a tradução da mensagem dos colegas.

Para avaliar a oficina, considerou-se essencial que, além da análise da professora responsável, os próprios alunos participassem da avaliação. Essa abordagem permite que os alunos acompanhem seu próprio desenvolvimento e se envolvam efetivamente no processo de ensino e aprendizagem.

Com esse objetivo, elaborou-se um questionário composto por perguntas abertas e fechadas. Algumas questões permitiam respostas mais detalhadas e argumentativas, enquanto outras eram dicotômicas, restringindo-se a respostas sim ou não. O objetivo das questões foi compreender como os alunos reagem a aulas que integram funções afins e criptografia de modo prático. O questionário foi aplicado aos alunos de ambas as turmas ao final da oficina, e os resultados serão apresentados separadamente para cada uma delas.

4 Resultados e discussão

Os resultados foram organizados com base nas respostas dos estudantes a cada pergunta

do questionário, sendo agrupados em tópicos para facilitar a compreensão e a análise.

Uso de Oficinas nas Aulas de Matemática

A primeira pergunta do questionário foi: “*A oficina contribuiu para o seu conhecimento sobre funções afins?*” As oficinas pedagógicas, por sua natureza, buscam transformar a aula em um espaço colaborativo de construção do conhecimento, rompendo com a lógica da mera transmissão de conteúdos.

Os alunos de ambas as turmas se mostraram receptivos à proposta metodológica. Todos responderam “Sim” à questão, indicando uma percepção positiva quanto à contribuição da atividade para a aprendizagem do conteúdo. A participação dos alunos e a compreensão do conteúdo abordado foram satisfatórias, com todos conseguindo codificar e decodificar suas mensagens ao final da oficina.

Embora a questão fosse discursiva, apenas alguns estudantes apresentaram justificativas. As respostas com argumentações mais detalhadas estão reunidas no Quadro 2.

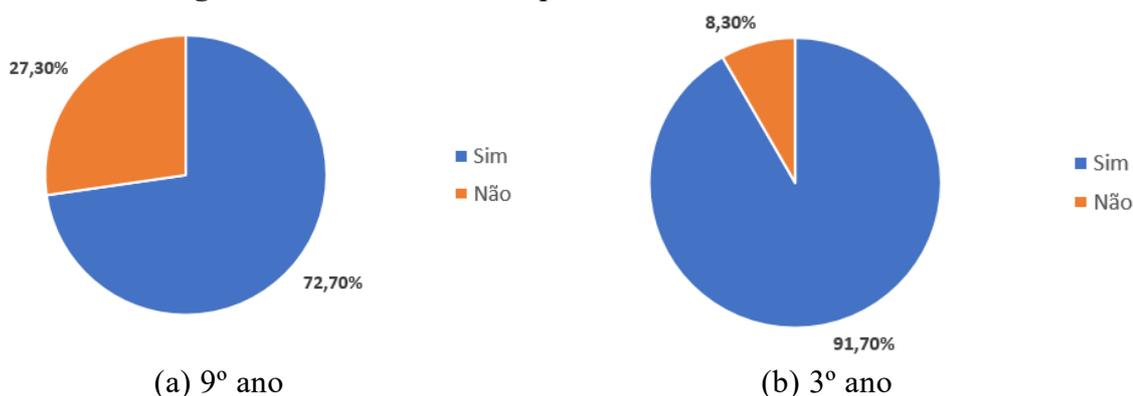
Quadro 2: Respostas justificadas da 1ª questão

9º ano
Sim, eu pude me aprofundar no assunto e pude entender mais.
Sim, aprendemos a descobrir mensagens e codificar.
3º ano
Sim, é uma forma mais divertida de aprendizado e o entendimento é melhor.
Sim, é bastante interessante para o aprofundamento da aprendizagem.
Sim, é muito legal colocar a mente para trabalhar o seu conhecimento.
Sim, contribuiu para o meu aprendizado.

Fonte: Autoras (2023)

Interesse dos Alunos pela História da Matemática

A segunda pergunta foi: “*Você gostou da utilização da história da matemática no desenvolvimento da oficina?*” Os resultados obtidos estão apresentados na Figura 1.

Figura 1: Nível de interesse pela história da matemática

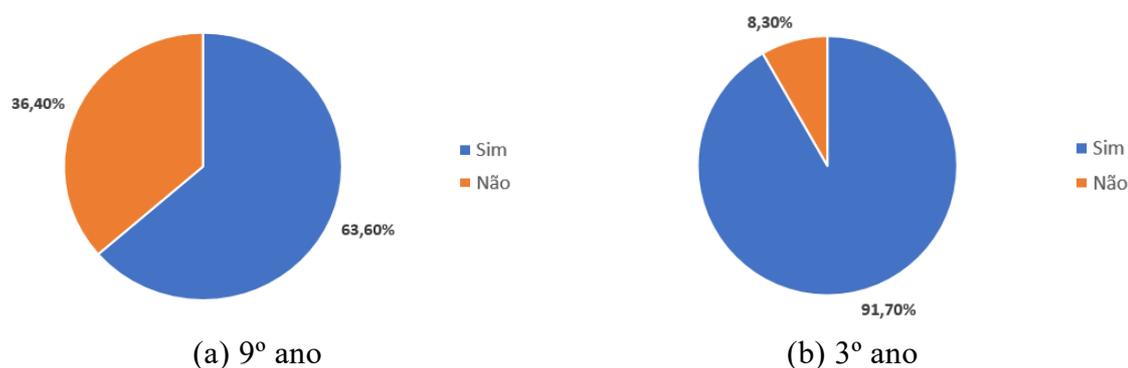
Fonte: Autoras (2023)

A matemática evoluiu ao longo da história para atender às necessidades dos povos, mas hoje ela chega às salas de aula em sua forma refinada, com definições, teoremas, propriedades e axiomas. Roque (2012, p. 20) observa que, em vez de apresentar um conceito matemático conforme seu desenvolvimento histórico e as questões que ele resolve, frequentemente tratamos o conceito como algo já pronto. Assim, o aluno tende a construir o conhecimento sem compreender, na maioria das vezes, sua origem ou relevância. Associar o estudo da matemática a contextos concretos ou contextualizados pode abrir novas possibilidades para a compreensão da disciplina. Oficinas são ferramentas pedagógicas que permitem aos docentes transformar a aula em um processo de construção coletiva de conhecimento, em vez de uma simples transferência de informações, promovendo a interação e troca entre os alunos.

Na oficina proposta, a história da criptografia foi abordada para que os alunos compreendessem o motivo da criação de códigos e seu funcionamento antes da era computacional. Conforme ilustrado na Figura 1, a aceitação dos alunos em relação à inclusão da história da matemática como base para o ensino e aprendizagem é elevado, especialmente na turma do 3º ano.

A Presença da Criptografia no Cotidiano

A oficina visou esclarecer o conceito e a aplicação da criptografia, uma vez que muitos alunos apenas conheciam o termo. Inclusive, foi solicitado que houvesse mais aulas práticas desse tipo. A terceira pergunta foi: “*Em algum momento você já tinha ouvido falar em criptografia?*” As respostas obtidas estão apresentadas na Figura 2.

Figura 2: Conhecimento prévio acerca da criptografia

Fonte: Autoras (2023)

Como evidenciado neste trabalho, a criptografia tem desempenhado um papel crucial na segurança das informações desde a Grécia Antiga, onde foi desenvolvida para proteger comunicações durante conflitos. Hinz (2000, p. 12) observa que, embora a criptografia mantenha uma grande importância militar, ela também é amplamente utilizada em diversas áreas que requerem segurança na transmissão de dados.

A Figura 2 revela que a palavra “criptografia” não é desconhecida, especialmente para a turma do 3º ano. Entre os alunos que já conheciam o termo, o conhecimento estava associado principalmente ao aplicativo *WhatsApp*. Quando questionados em sala de aula sobre o funcionamento da criptografia antes da apresentação, os alunos não chegaram a um consenso sobre como ela operava, apenas reconheceram que se tratava de códigos. A oficina foi, portanto, bastante útil para esclarecer esses conceitos.

Destaca-se aqui a importância de se desenvolver oficinas baseadas no cotidiano dos alunos a fim de oferecer uma abordagem prática e envolvente para o aprendizado, permitindo que os conceitos formais se conectem diretamente com a realidade dos estudantes. Ao integrar um tema já ouvido pelos alunos no seu dia a dia, a oficina tornou o conteúdo de funções afins mais relevante e acessível, facilitando a compreensão e a aplicação dos conceitos teóricos. Assim, a criptografia pode estimular o interesse e a motivação dos alunos, promovendo uma aprendizagem mais significativa e duradoura e contribuindo para o desenvolvimento de habilidades práticas e a construção de conhecimento contextualizado.

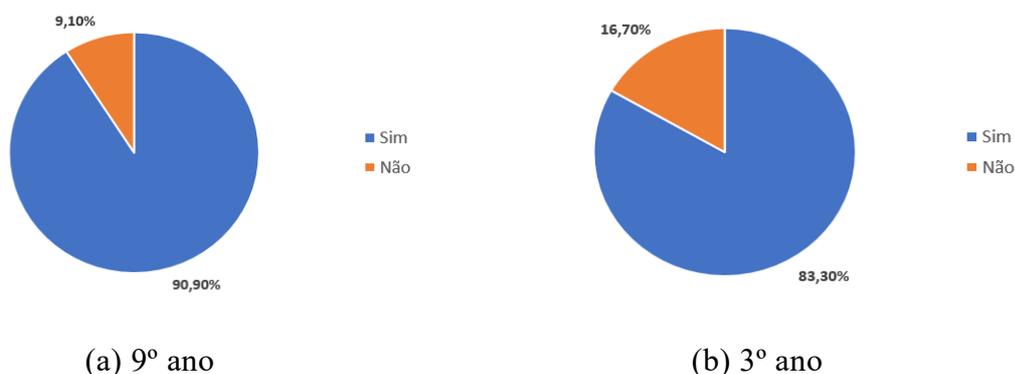
Interesse pela Criptografia

A criptografia está presente em diversas plataformas utilizadas no dia a dia, como redes sociais, e-mails e sistemas bancários. Embora os alunos a utilizem de forma implícita, a oficina

visou evidenciar a relevância da criptografia na vida cotidiana, oferecendo uma base para um estudo mais aprofundado do tema e estimulando o interesse dos alunos em expandir seu conhecimento. Como destaca Hagemeyer (2004, p. 81), “o que o aluno aprende transcende a sala de aula, conferindo ao trabalho do professor um impacto significativo na formação dos indivíduos”.

Diante dessa proposta de ampliar o interesse pelo tema e promover conexões com o cotidiano dos alunos, investigou-se se a oficina despertou a vontade de aprofundar os conhecimentos sobre criptografia. Para isso, formulou-se a quarta pergunta: “*A oficina despertou algum interesse para se aprofundar no assunto?*”, cujas respostas estão representadas na Figura 3.

Figura 3: Interesse pela criptografia



Fonte: Autoras (2023)

Os resultados apresentados na Figura 3, quando comparados com os dados da Figura 2 sobre o conhecimento prévio dos alunos, indicam que o 9º ano apresentou maior interesse em continuar estudando criptografia após a oficina. Isso pode ser atribuído ao fato de que esses alunos tinham um conhecimento inicial mais limitado sobre o tema.

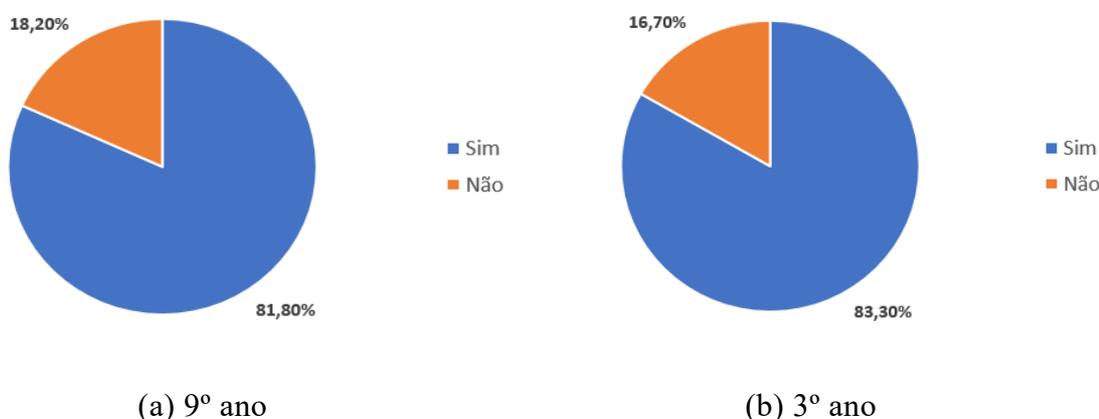
Embora o conhecimento sobre criptografia seja relevante para o cotidiano dos alunos, frequentemente é negligenciado, apesar de seu acesso a uma vasta gama de informações. Isso ocorre, muitas vezes, devido à falta de uma educação digital eficaz, que deveria não apenas introduzir a tecnologia, mas também integrá-la de maneira significativa ao processo de aprendizado.

Conclusões dos Alunos sobre a Criptografia

A última pergunta foi a seguinte: *Sua concepção sobre o que é criptografia e de como funciona mudou ao final da oficina? Justifique.* Esta questão permitia respostas mais

elaboradas, com comentários e explicações.

Figura 4: Parecer dos alunos sobre o quanto aprenderam na oficina



Fonte: Autoras (2023)

Com base na Figura 4, observa-se uma paridade entre os grupos quanto à compreensão da criptografia. A análise revelou que, de maneira geral, a oficina contribuiu para um entendimento mais claro do conceito de criptografia pelos alunos. O Quadro 3 apresenta excertos das respostas fornecidas pelos alunos.

Quadro 3: Recorte de respostas afirmativas relativas à 5ª questão

9º ano
Sim, a criptografia é bem mais interessante e divertida do que parece ser.
Sim, não sabia o que era criptografia e foi bom, porque é mais um conhecimento.
Sim, as funções que foram passadas nos ajudam a realizar exercícios em sala de aula.
3º ano
Sim, eu já tinha um pouco de conhecimento sobre o assunto, mas oficina melhorou.
Sim, despertou-me ainda mais interesse sobre o assunto.
Sim, porquê com a criação das mensagens o conteúdo ficou bem mais interessante.

Fonte: Autoras (2023)

Para o 9º ano, as respostas foram predominantemente positivas. Mesmo os alunos que indicaram não ter uma mudança de concepção afirmaram que a oficina contribuiu para o seu conhecimento sobre criptografia. Aqueles que responderam afirmativamente destacaram que o tema se mostrou divertido e interessante. Em contraste, no 3º ano, uma resposta negativa foi atribuída ao fato de um aluno já possuir conhecimento prévio sobre o assunto e estar familiarizado com o funcionamento da criptografia.

Avaliação da professora que desenvolveu a oficina

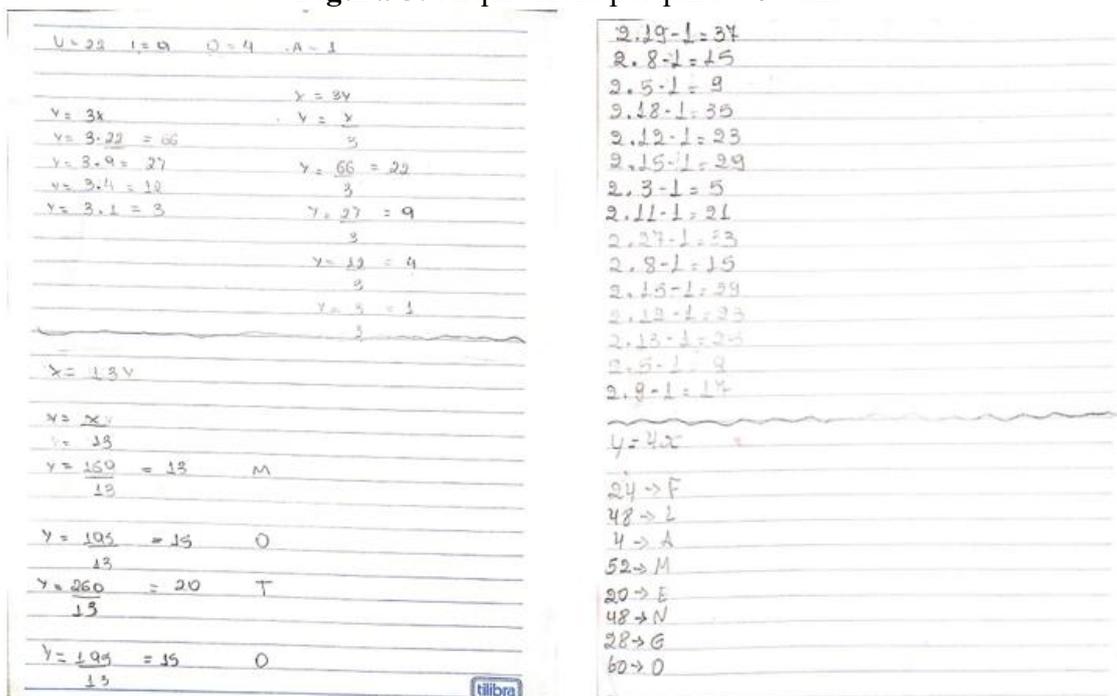
Muitos estudantes percebem as aulas de matemática como monótonas. Construir projetos que atendam aos interesses individuais dos alunos é desafiador, dado que cada um possui suas próprias singularidades. O papel do educador é incentivar a capacidade dos alunos de gerar ideias, comunicá-las e implementá-las na prática.

A oficina foi bem recebida pela maioria dos estudantes. Todos os grupos conseguiram entregar suas mensagens ao final e decifrar as dos colegas. Como relataram em seus questionários, muitos alunos consideraram a experiência uma forma interessante de aprender e aplicar o conteúdo de funções afins.

Embora os resultados do questionário tenham sido similares em ambas as turmas, observou-se um comportamento distinto em sala de aula. Os alunos do 9º ano mostraram maior engajamento, concluindo as atividades antes do prazo e mostrando particular interesse pelos aspectos históricos da criptografia, com frequentes questionamentos. Esse entusiasmo persistiu mesmo diante das dificuldades iniciais nos cálculos matemáticos, evidenciando sua receptividade às tarefas propostas.

A Figura 5 exibe mensagens criptografadas pela turma, com palavras que refletem seu cotidiano e interesses, como “MOTO” e “FLAMENGO”. Esse cenário evidencia como o tema da criptografia pode aproximar a matemática da realidade dos alunos.

Figura 5: Arquivos da pesquisa – 9º ano



Fonte: Autoras (2023)

No início da oficina, a turma do 3º ano mostrou-se desatenta, o que se refletiu na produção e, especialmente, na decodificação das mensagens. Os estudantes frequentemente apresentavam dificuldade em manter o foco, tornando o ambiente de aprendizagem um desafio constante para a concentração. Alguns alunos conseguiram concluir as tarefas apenas no prazo final. É possível que a incorporação de elementos tecnológicos na atividade, como o uso de *softwares* para criptografia, pudesse aumentar o interesse e a participação desses estudantes.

A atividade visava introduzir o conceito de criptografia e consolidar o conhecimento sobre funções afins, além de observar como os alunos abordam a criação e resolução de problemas. Como destaca Hinz (2000, p. 23), “Quando o aluno estuda técnicas para criptografar mensagens [...] através de permutações, funções, matrizes, entre outros, ele visualiza situações reais e consegue chegar mais facilmente a um resultado.” A maioria dos estudantes reconheceu que as oficinas facilitaram a assimilação do conteúdo matemático e solicitaram a realização de mais aulas desse tipo. A rotina diária em sala de aula pode tornar o processo de ensino e aprendizagem monótono; entretanto, a inclusão de projetos práticos pode tornar a experiência mais envolvente e estimulante.

De modo geral, o questionário aplicado após a oficina revelou que os alunos compreendem o tema, embora nem todos tenham manifestado interesse em se aprofundar no assunto. Inicialmente, o termo “criptografia” causou certa apreensão entre os estudantes; no entanto, à medida que a oficina avançava, eles passaram a entender que o funcionamento da criptografia é acessível. Compreendeu-se que a criptografia é um sistema de algoritmos, existente há muitos anos, que opera por meio do embaralhamento de informações e que, com o tempo, a decodificação de mensagens criptografadas tornou-se cada vez mais complexa devido ao avanço tecnológico e à implementação de técnicas matemáticas sofisticadas.

Considerações finais

A oficina proposta por Miranda e Paula (2021), que utiliza a criptografia como tema motivador para o ensino e a aprendizagem de funções afins, foi desenvolvida em duas turmas. O objetivo foi despertar o entusiasmo dos alunos, aproveitando a atualidade e a relevância do tema no cotidiano. Diversas pesquisas nas áreas da Educação Matemática e da Matemática abordam a integração de temas contemporâneos para enriquecer o processo educativo e tornar o aprendizado mais envolvente e significativo.

Apesar da complexidade dos métodos criptográficos modernos, a oficina buscou ilustrar seu funcionamento por meio de um exemplo simples com o uso de funções afins. A

proposta foi evidenciar aos professores de matemática que o tema pode ser abordado de maneira acessível desde o Ensino Fundamental, facilitando a compreensão e despertando o interesse dos alunos por conceitos matemáticos aplicados a situações reais.

Para promover maior envolvimento dos alunos com atividades relacionadas à criptografia, a oficina evidenciou que, conforme sugerido por Miranda e Paula (2021), é benéfico que o professor integre a história, os conceitos e as aplicações do tema. Essa abordagem ajuda a conectar a criptografia ao conteúdo matemático, favorecendo uma aprendizagem mais efetiva.

Assim, com base nas respostas obtidas por meio do questionário aplicado, conclui-se que o objetivo de permitir aos alunos a assimilação do conceito de criptografia, da sua forma de funcionamento e do seu papel histórico na humanidade foi alcançado.

Como sugestão para trabalhos futuros, considerando o menor envolvimento dos alunos do 3º ano do Ensino Médio, recomenda-se adaptar a oficina com a utilização de *softwares*. A integração de ferramentas tecnológicas pode ajudar a despertar um maior interesse e engajamento desses alunos com o tema da criptografia.

Por fim, espera-se que este trabalho auxilie e inspire docentes em suas práticas pedagógicas, pois a criptografia pode servir como uma ponte eficaz entre teoria e realidade. Ao integrar temas como a criptografia nas aulas de matemática, os professores têm a oportunidade de tornar o ensino mais relevante e envolvente, promovendo uma aprendizagem mais significativa e eficaz.

Referências

- ALMOULOU, S. A.; FIGUEROA, T. P.; FONSECA, R. V. Análise epistemológica de teoria dos números e criptografia: importância dessas áreas nos currículos de licenciatura em Matemática. **Revista Paranaense de Educação Matemática**, Campo Mourão, v. 10, n. 21, p. 22-43, 2021.
- BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, 2018.
- GALDINO, U. E. **Teoria dos números e criptografia com aplicações básicas**. 2014. Dissertação (Programa de Pós-Graduação Profissional em Matemática – Profmat) – Centro de Ciências e Tecnologia. Universidade Estadual da Paraíba. Campina Grande. 2014.
- HAGEMEYER, R. C. C. Dilemas e desafios da função docente na sociedade atual: os sentidos da mudança. **Educar em Revista, Curitiba**, v. 20, n. 24, p. 67-85, 2004.
- HINZ, M. A. M. **Um estudo descritivo de novos algoritmos de criptografia**. 2000. Monografia (Curso de Bacharelado em Informática) – Instituto de Física e Matemática, Universidade Federal de Pelotas. Pelotas. 2000.

KRANZ, B. E.; OLGIN, C. A. Construção de conhecimentos matemáticos utilizando a temática criptografia para o Ensino Médio. **Revista de Ensino de Ciências e Matemática**, São Paulo, v. 12, n. 3, p. 1-21, 2021.

MENEZES, R. **Criptografia e álgebra**. 2013. Monografia (Curso de Matemática) – Departamento de Matemática, Universidade Federal de Minas Gerais. Belo Horizonte. 2013.

MIRANDA, A. A. N. S.; PAULA, F. V. Uma proposta para o ensino de funções afins por meio da criptografia. **REAMEC – Rede Amazônica de Educação em Ciências e Matemática**, Cuiabá, v. 9, n. 2, p. 1-22, 2021.

OLGIN, C. A.; GROENWALD, C. L. O. Engenharia Didática: uma experiência com o tema criptografia. **Jornal Internacional de Estudos em Educação Matemática**, São Paulo, v. 4, n. 2, p. 158-190, 2011.

REIS, V. L. M. **Criptografia, segurança de dados e privacidade**. 1989. Tese (Curso de Engenharia) – Instituto de Matemática, Universidade Federal do Rio de Janeiro. Rio de Janeiro. 1989.

RODRIGUES, L. P. O.; SÁ, L. C. Matrizes e Criptografia: contribuições de uma atividade sobre o Whatsapp no Ensino Médio. **Revista de Ensino de Ciências e Matemática**, São Paulo, v. 10, n. 6, p. 255-273, 2019.

ROQUE, T. **História da matemática**: Uma visão crítica, desfazendo mitos e lendas. Rio de Janeiro: Zahar, 2012.