Educação Matemática

UMA PROPOSTA PARA O ENSINO DE FUNÇÕES AFINS POR MEIO DA CRIPTOGRAFIA

A PROPOSAL FOR THE TEACHING OF AFIM FUNCTIONS THROUGH CRIPTOGRAPHY

UNA PROPUESTA PARA LA ENSEÑANZA DE FUNCIONES AFINES MEDIANTE LA CRIPTOGRAFÍA

Noronha de Sousa Miranda, Ariane Andressa; Vital de Paul, Fernanda

Ariane Andressa Noronha de Sousa Miranda *
ariane.andressa@mail.uft.edu.br
Universidade Federal do Tocantins, Brasil

Fernanda Vital de Paul **
fernandavital@uft.edu.br
Universidade Federal do Tocantins, Brasil

REAMEC – Rede Amazônica de Educação em Ciências e Matemática
Universidade Federal de Mato Grosso, Brasil
ISSN-e: 2318-6674
Periodicidade: Frecuencia continua
vol. 9, núm. 2, e21059, 2021
revistareamec@gmail.com

Recepção: 21 Junho 2021
Aprovação: 02 Agosto 2021
Publicado: 28 Agosto 2021

URL: http://portal.amelica.org/ameli/jatsRepo/437/4372405029/index.html

DOI: https://doi.org/10.26571/reamec.v9i2.12652

Resumo: Diante da perspectiva de que a Matemática deve ser ensinada de forma a produzir significado por meio de situações que remetam à realidade do aluno, esse artigo propõe a inserção da criptografia no 9º ano do Ensino Fundamental por meio de uma oficina, tratando-se de um recorte do trabalho de conclusão de Curso de uma das autoras. A oficina proposta visa uma breve recapitulação acerca da história e funcionamento da criptografia e a abordagem de um método criptográfico praticável no Ensino Básico, utilizando funções afins. Para a exposição da mesma, o artigo lança mão da pesquisa qualitativa, de cunho bibliográfico, com o objetivo de embasar a aplicação e desenvolvimento da oficina em sala de aula pelo professor. Dessa forma, a história da criptografia será brevemente apresentada bem como seus principais conceitos e alguns métodos, seguindo para a apresentação da oficina por meio da metodologia utilizada para sua organização, que consiste em três momentos distintos: abordagem histórica, exemplificação/revisão de conteúdo e prática.

Palavras-chave: Criptografia, Oficina, Função Afim, Matemática, Ensino Fundamental.

Abstract: Given the perspective that Mathematics should be taught in order to produce meaning through situations that refer to the student's reality, this article proposes the insertion of cryptography in the 9th year of Elementary School through a workshop, dealing with an excerpt from one of the authors' course conclusion work. The proposed workshop aims at a brief recapitulation about the history and functioning of cryptography and the approach of a practicable cryptographic method in Basic Education, using affine functions. For the exposition of the same, the article makes use of qualitative research, of bibliographic nature, with the objective of supporting the application and development of the workshop in the classroom by the teacher. Thus, the history of cryptography will be briefly presented, as well as its main concepts and some methods, followed by the presentation of the workshop through the methodology used for its organization, which consists of three distinct moments: historical approach, ilustration/ review of contet and practice.

Keywords: Cryptography, Workshop, Affine Function, Mathematics, Elementary School.

Resumen: Dada la perspectiva de que la Matemática debe enseñarse para producir significado a través de situaciones que remitan a la realidad del alumno, este artículo propone la inserción de la criptografía en el 9 ° año de Educación Primaria a través de un taller, abordando un fragmento de la obra de uno de los autores. trabajo de conclusión del curso. El taller propuesto tiene como objetivo una breve recapitulación sobre la historia y el funcionamiento de la criptografía y el enfoque de un método criptográfico practicable en Educación Básica, utilizando funciones relacionadas. Para la exposición de los mismos, el artículo hace uso de una investigación cualitativa, de carácter bibliográfico, con el objetivo de apoyar la aplicación y desarrollo del taller en el aula por parte del docente. Así, se presentará brevemente la historia de la criptografía, así como sus principales conceptos y algunos métodos, seguido de la presentación del taller a través de la metodología utilizada para su organización, que consta de tres momentos diferenciados: enfoque histrico, ilustracin/ revisin de contenido y practica.

Palabras clave: Criptografía, Taller, Función afín, Matemáticas, Enseñanza fundamental.

1. INTRODUÇÃO

O educador, ao utilizar estratégias e metodologias de ensino que interligam o conhecimento matemático com situações reais, reforça e desenvolve a habilidade de raciocínio do aluno e competências como a capacidade de resolver problemas, a criatividade e a liberdade no processo de aprendizagem que convergem para a concepção de um pensamento lógico. Dessa forma, tal percepção faz-se necessária desde os primeiros anos do Ensino Básico, como reforça as normas da Base Nacional Comum Curricular (BNCC):

> O Ensino Fundamental deve ter compromisso com o desenvolvimento do letramento matemático, definido como as competências e habilidades de raciocinar, representar, comunicar e argumentar matematicamente, de modo a favorecer o estabelecimento de conjecturas, a formulação e a resolução de problemas em uma variedade de contextos, utilizando conceitos, procedimentos, fatos e ferramentas matemáticas. É também o letramento matemático que assegura aos alunos reconhecer que os conhecimentos matemáticos são fundamentais para a compreensão e a atuação no mundo e perceber o caráter de jogo intelectual da matemática, como aspecto que favorece o desenvolvimento do raciocínio lógico e crítico, estimula a investigação e pode ser prazeroso (fruição) (BRASIL, 2018, p.266).

Diante desta perspectiva de que a Matemática deve ser ensinada de forma a produzir significado por meio de situações que remetam à realidade do aluno, esse artigo se baseia na criptografia, que é vista aqui como potencial despertadora do interesse dos alunos, por sua grande presença no cotidiano e relação com o mundo contemporâneo no que diz respeito ao sigilo de informações discutido no uso cada vez mais frequente de recursos tecnológicos. Neste sentido Pereira (2015, p. 13) afirma, "Fazer com que o aluno consiga atribuir a

Autor notes

* Graduação em Licenciatura em Matemática (UFT). Professora do Colégio Estadual José Luiz Siqueira (CEJLS), Wanderlândia, TO, Brasil. Endereço para correspondência: Av. Lontra, 448, bairro JK, Araguaína, TO, Brasil, CEP: 77816-190.

** Doutorado em Estatística (UFPE). Professora da Universidade Federal do Tocantins (UFNT), Araguaína, TO, Brasil. Endereço para correspondência: Av. Paraguai, s/n, Setor Cimba, Araguaína, TO, Brasil, CEP: 77824-838.

real importância da temática, elencar os aspectos históricos e também saber contextualizar o que está sendo discutido é de fundamental importância no processo de ensino aprendizagem".

Acreditando ainda que o trabalho do professor não deve se restringir a uma única estratégia de ação, tendo em vista que quanto mais possibilidades de utilização de diversos tipos de abordagem, mais rico será o desenvolvimento dos mais variados temas que venha a se trabalhar com os alunos, este trabalho sugere a inserção da criptografia no Ensino Básico por meio de oficinas.

Entre as diversas ferramentas que podem ser utilizadas pelos docentes com o intuito de que a aula não seja puramente uma transferência de informações, as oficinas podem ser promissoras na construção coletiva de saberes, na promoção de troca de conhecimentos entre os próprios alunos e na desmistificação da Matemática como uma área que apresenta dificuldade de assimilação. Neste sentido, de acordo com Brasil (2018, p. 26), "Apesar de a Matemática ser, por excelência, uma ciência hipotético-dedutiva, [...] é de fundamental importância também considerar o papel heurístico das experimentações na aprendizagem da Matemática".

Portanto, este artigo tem como objetivo principal a proposição de uma oficina que tem como ponto central a utilização de funções afins para codificar e decodificar mensagens, de modo que os alunos se sintam motivados em desenvolverem seu conhecimento e entendam o funcionamento e a importância da criptografia de uma maneira simples, embora na prática criptográfica sejam utilizadas técnicas e conceitos complexos.

> Diferente de outras aplicações que requerem um grande conteúdo, pode-se iniciar os estudos com criptografia com conceitos elementares como a contagem. Porém o embasamento matemático não fica em conteúdos básicos, partindo desta aplicação, o professor pode atingir os maiores problemas da atualidade, que são estudados nos departamentos de matemática pura (BORGES, p. 822).

De modo geral, a oficina proposta contará com três momentos distintos. A princípio, a criptografia será contextualizada por meio de sua história. Posteriormente, a definição de funções e seus conceitos serão apresentados ou revistos utilizando exemplos criptográficos e, para finalizar, serão efetuadas trocas de mensagens secretas dentro de uma turma.

Antes de relatar o desenrolamento da função sugerida, serão apresentados os principais fatos históricos no desenvolvimento da criptografia, assim como os conceitos abarcados pelo tema como chaves e métodos criptográficos. Alguns conceitos matemáticos também serão lembrados, quando necessário, para o desenvolvimento e entendimento do processo de ciframento e decodificação de mensagens em exemplos que serão exibidos. Para tal, lança-se mão da pesquisa qualitativa, de cunho bibliográfico.

2. CRIPTOGRAFIA: HISTÓRIA E MÉTODOS

No cotidiano, muitas informações devem ser mantidas em sigilo e/ou disponíveis ao acesso de poucos. Alguns exemplos são conversas em aplicativos de mensagens, transações bancárias, e-mails, informações militares, dados de clientes e outros. Pela necessidade de segurança nas informações que remota de tempos mais distantes, nasceu a criptografia.

Nesta seção, será apresentada uma breve história da criptografia, onde os interessados em desenvolver a oficina proposta poderão se pautar para a contextualização histórica sugerida. Também serão apresentados alguns métodos criptográficos como o RSA e a cifra de Hill.

2.1. Breve história da criptografia

A palavra criptografia vem do grego kriptos (escondido) e grapho (escrita), caracterizando-se como um mecanismo de codificação da escrita. Seu objetivo é que uma determinada mensagem seja recebida apenas pelo seu legítimo destinatário e esse, com o uso de uma chave específica, possa ter acesso a ela.

A criptografia foi desenvolvida em períodos de guerra, oriunda da necessidade de ocultação de dados para garantir estratégias, vantagens e segurança de vidas, tesouros e terras. Menezes (2003, p. 15) diz que "[...] a ameaça de interceptação de mensagens por espiões motivou não apenas o desenvolvimento de métodos para torná-las ininteligíveis, mas também o aparecimento de técnicas para ocultá-las". A ação de criptografar funciona como um sistema de algoritmos embaralhando o conteúdo, possuindo as fases de codificação e decodificação. Codificar é converter os componentes de uma mensagem em símbolos secretos por meio de um algoritmo. O processo também é chamado de encriptação ou ciframento.

Sobre seu início, Galdino (2014, p. 5) destaca "Uma das primeiras informações data de Heródoto no ano de 480 a.C., o qual escreveu sobre os conflitos entre Grécia e a Pérsia". Posteriormente, o imperador Júlio César em, aproximadamente, 50 a.C., usou um método para confabular com os seus generais, o qual consistia na troca de todas as letras dos seus comunicados. Dessa forma, mesmo que interceptadas pelos inimigos, as mensagens enviadas e recebidas iriam parecer sem significado. A técnica consistia em transpor as letras do alfabeto que eram substituídas por letras localizadas em outras posições, seguindo espaçamentos determinados. Levando o nome do seu criador, esse método ficou conhecido como cifra de César. A Figura 1 ilustra o funcionamento da transposição, por meio de um exemplo onde cada letra do alfabeto é substituída pela letra posicionada à sua frente em três casas.

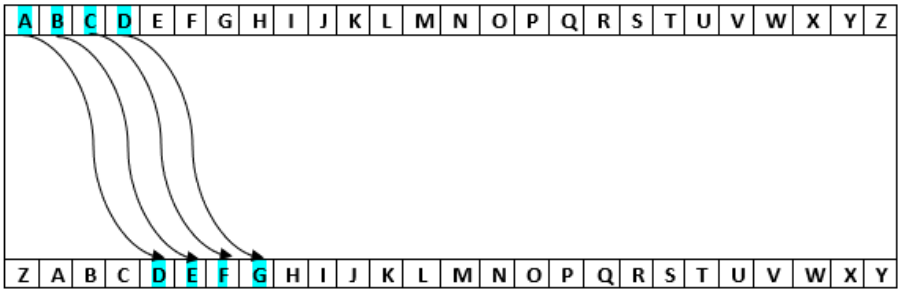


FIGURA 1
Exemplo da cifra de César
Fonte: Autoras

A partir da segunda guerra mundial, a criptografia passou a ser usada de forma extensa em todas as ações. Neste contexto, é importante dar destaque à máquina Enigma, criada pelo engenheiro alemão Arthur Scherbius no fim da primeira guerra é exibida na Figura 2. Manipulada a partir de 1920 pelo governo e para fins militares, a máquina possibilitava que a Alemanha trocasse informações sobre ataques e localizações. A criptografia da Enigma era simples, mas sua engrenagem gerava milhares de possibilidades de mensagens criptografadas, impossíveis de serem decifradas naquela época.

FIGURA 2
Máquina Enigma
Fonte: Pereira (2015)

Em 1939, Alan Turing se juntou a um grupo de matemáticos para trabalhar no Government Code and Cypher School no Reino Unido, com o objetivo de decifrar diariamente os códigos alemães. Turing insistiu na produção da máquina eletromecânica, chamada Bombe, com o objetivo de capturar e decifrar as mensagens criptografadas pela Enigma. A Bombe, exibida pela Figura 3, foi essencial para a derrota nazista na guerra.

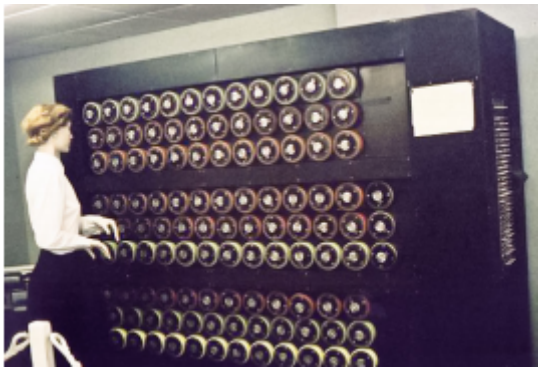


FIGURA 3
Máquina Bombe
Fonte: Paixão (2020)

O trabalho de Turing foi uma das inspirações para o surgimento dos computadores. Neste sentido, ainda no século XX, "A máquina britânica foi criada pelo matemático Max Newman que, se baseando na máquina de Turing, criou a Colossus, um invento capaz de se adaptar a diferentes problemas, o que na atualidade chamaríamos de computador programável" (PAIXÃO, 2020, p.53).

Conforme Groenwald et al., depois da segunda guerra mundial a área da criptografia realmente cresceu com o desenvolvimento dos computadores, quando foram realizados diversos estudos de complexos algoritmos matemáticos, que formaram a base para a ciência da computação moderna.

> Hoje, a criptografia continua tendo uma importância militar ainda muito grande, entretanto ela é usada também nas mais diversas áreas onde a transmissão de dados necessita de segurança. A crescente necessidade de métodos criptográficos mais seguros foi alavancada principalmente pelo aumento da quantidade de informação armazenada e pela expansão das redes de computadores (HINZ, 2000, p.12).

Hodiernamente, houveram melhorias na segurança e na complexidade dos métodos utilizados para cifrar e decifrar mensagens na criptografia. Esse aperfeiçoamento está associado à internet, que exigiu a transferência

de informações entre computadores e outros dispositivos conectados à rede que não podem ser acessadas por partes não interessadas diretamente.

2.2. Métodos criptográficos

Para a utilização dos métodos criptográficos faz-se necessário o uso de chaves. De acordo com essas chaves, a criptografia classifica-se como simétrica ou assimétrica. No primeiro caso, utiliza-se uma chave única para cifrar e decifrar a mensagem e, no segundo, opera-se com um duo de chaves, uma pública e outra privada, que se relacionam por meio de um algoritmo.

Na criptografia simétrica, cujo funcionamento é ilustrado pela Figura 4, a chave é usada junto com o algoritmo de ciframento que envia uma mensagem cifrada e está poderá ser decodificada, caso o receptor saiba o algoritmo de deciframento correspondente e tenha a mesma chave.

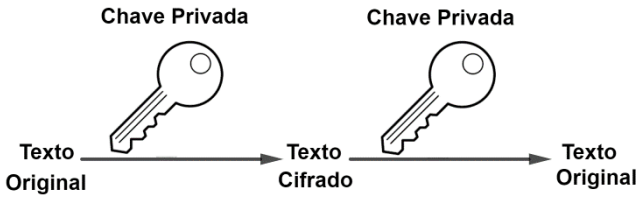


FIGURA 4
Representação da criptografia simétrica
Fonte: Autoras

Nesse caso, tem-se o benefício da praticidade, sendo possível criptografar uma quantidade maior de dados em menos tempo. Sua desvantagem é que se algum interceptor conseguir a chave, conseguirá acessar a mensagem.

A criptografia assimétrica utiliza duas chaves diferentes, uma pública e outra privada, como representado pela Figura 5. Nesta, somente a primeira codifica e apenas a segunda decodifica.

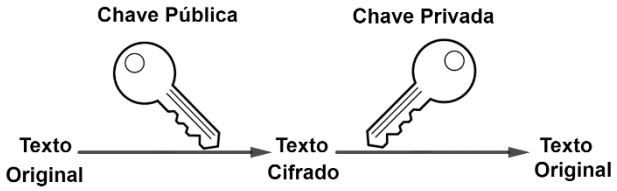


FIGURA 5
Conceito do funcionamento da criptografia assimétrica
Fonte: Autoras

A chave pública pode ser conhecida por diversos usuários, já a privada é de uso exclusivo. A criptografia assimétrica é utilizada em aplicativos de troca de mensagens e sua principal vantagem é que, caso o interceptor possua acesso à chave pública, ele só consegue descriptografar os dados com a obtenção da chave privada, que

é de uso particular do receptor e em nenhum momento precisa ser compartilhada. A desvantagem é que o processo de criptografar se torna mais longo, graças ao uso de algoritmos mais complexos.

Alguns dos métodos ou algoritmos criptográficos que permitem cifrar mensagens são os seguintes: transposição, substituição ou ciframento composto. A transposição é realizada pela reorganização das letras e pode ser feita de inúmeras maneiras. Já a substituição pode ser monoalfabética (onde cada letra é substituída sempre pela sua correspondente, independentemente de quantas vezes aparece) e polialfabética (a mesma letra no texto pode ser trocada por variações). No caso do ciframento composto, usa-se transposição e substituição, sendo um padrão usado em ambientes computacionais.

2.2.1. Criptografia RSA

Como já manifestado, a criptografia moderna não é simples como a cifra de César, por exemplo, que utiliza o método de transposição. Hoje, ao invés de letras, utiliza-se números binários em computadores para proteger transações bancárias, senhas de e-mails e redes sociais.

Diante da realidade tecnológica, as empresas passaram a investir em ferramentas de segurança, utilizando a criptografia RSA. Esse método é composto por diferentes algoritmos assimétricos resultando em uma encriptação mais segura. Seu funcionamento é baseado em princípios matemáticos, utilizando números primos. Galdino (2014, p.61) assegura "A garantia de segurança está relacionada com a dificuldade na fatoração do produto de dois números primos relativamente grandes". Por esse motivo, a descriptação torna-se inviável até para uma máquina.

Para um melhor entendimento da criptografia RSA, cujo aprofundamento não será dado neste artigo, Coutinho (2015) pode ser consultado.

2.2.2. Cifra de Hill

A cifra de Hill foi criada por Lester Hill, em 1929. Trata-se de um algoritmo de substituição fundamentado na Álgebra Linear. Pereira et al. (2012, p.4) diz que "o processo de cifras de Hill consiste em transformar pares sucessivos de texto em texto cifrado, através da escolha de uma matriz de ordem que precisa ser invertível e uma tabela com valores numéricos para todas as letras do alfabeto".

Outras ordens para podem ser utilizadas, desde que a matriz também seja inversível. Utilizando a notação de matrizes para representar este algoritmo, tem-se:

$C = \mathrm{AM}$

onde é a matriz com as letras da mensagem original , a matriz é chave do ciframento e é a mensagem codificada $(c_1, ..., c_n)$, isto é,

Na forma de sistemas lineares, tem-se:

Para decifrar uma mensagem, isto é, obter **M**, sendo **A** inversível, faz-se $M = A^{-1}C$.

2.3. Considerações acerca da matemática envolvida nos métodos criptográficos

No contexto do Ensino Básico, alguns conteúdos da disciplina de Matemática podem ser abordados por meio da criptografia, mediante o desenvolvimento de oficinas em sala de aula. Tendo em vista a aplicabilidade da criptografia no mundo real, os alunos teriam a oportunidade de aproximar a teoria da prática e terem seus interesses despertados para a disciplina.

Acerca dos conteúdos que podem ser abordados, estes dependem do método criptográfico que seria contemplado e a qual ano do Ensino Básico a oficina seria direcionada. Nesta perspectiva, o Quadro 1 apresenta algumas possibilidades que associam o ano do Ensino Básico, aos objetos de conhecimento previstos na BNCC e ao método criptográfico que permitem a abordagem de tais objetos.

QUADRO 1
Possibilidades para o ensino de criptografia no Ensino Básico.

Público Alvo	Conteúdo	Método
8° do Ensino Fundamental	Equações e Potenciação	Cifra de substituição
9° do Ensino Fundamental	Função linear	
1° ano Ensino Médio	Funções: quadráticas, exponenciais e logarítmicas	
2° ano Ensino Médio	Análise combinatória	
5° ano do Ensino Fundamental	Números primos e fatoração	Método RSA
6° ano do Ensino Fundamental	Múltiplos e divisores de um número natural e Números primos e compostos	
7° ano do Ensino Fundamental	Múltiplos e divisores de um número inteiro	
9° ano do Ensino Fundamental	Funções	Cifra de Hill
2° ano Ensino Médio	Matrizes	

Fonte: Autoras.

A oficina que será proposta nesse artigo está associada a segunda e penúltima linha do Quadro 1, sendo direcionada ao 9° ano do Ensino Fundamental. Para compreensão da matemática envolvida na cifra de Hill e de sua adaptação ao uso de funções invertíveis ao invés de matrizes invertíveis, seu funcionamento será apresentado, bem como algumas definições, propriedades e teoremas envolvendo funções.

2.3.1. A cifra de Hill e matrizes

Originalmente a cifra de Hill baseia-se em um sistema de transformações matriciais, utilizando conceitos da Álgebra Linear como determinante, multiplicação, identidade e cálculo das inversas de matrizes.

Por meio de um exemplo, tal método será exposto. O primeiro passo para a utilização do método é ter uma correspondência entre letras e números, tal como exibido pelo Quadro 2.

QUADRO 2
Correspondência entre letras e números

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

Fonte: Autoras

Posteriormente, faz-se necessário a definição de uma chave que, neste caso, deve ser uma matriz invertível. No exemplo a seguir, a matriz posteriormente exibida será utilizada como chave.

$$\begin{bmatrix} 1 & 2 \\ 0 & 4 \end{bmatrix}$$

O objetivo será a cifragem da mensagem sigilo. Para tal, cada letra será substituída por sua letra correspondente, conforme o Quadro 2, obtendo a sequência:

19 – 9 – 7 – 9 – 12 – 15.

Fazendo a multiplicação de matrizes de acordo com a equação $C = AM$, sendo a matriz referente a cada um dos blocos si, gi, lo, isto é, $\begin{bmatrix} 19 \\ 9 \end{bmatrix}$, $\begin{bmatrix} 7 \\ 9 \end{bmatrix}$, $\begin{bmatrix} 12 \\ 15 \end{bmatrix}$ e **A**, a matriz indicada pela chave respectivamente, obtém-se:

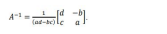
Logo, a mensagem cifrada conforme a correspondência entre números e letras e a chave utilizada, é dada por:

37 – 36 – 25 – 36 – 42 – 60.

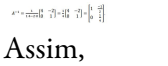
Caso o objetivo seja descobrir a mensagem original, a partir da cifrada, a equação $M = A^{-1}C$ deve ser utilizada. Para isso, faz-se necessária a obtenção de A^{-1}, ou seja, a matriz inversa de A, de modo que a matriz A de tamanho **2 x 2**, sendo:

$$A = \begin{bmatrix} a & b \\ c & c \end{bmatrix},$$

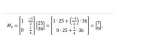
é invertível se, e somente se, $ad - bc \neq 0$. Nesse caso, tem-se:



Para o exemplo considerado, segue que:



Assim,



Observando os conceitos envolvidos no exemplo apresentado, o mesmo seria adequado aos alunos do 2º ou 3º ano do Ensino Médio, tendo em vista que o conteúdo de matrizes está previsto no 2#º ano. A fim de adaptar a cifra de Hill de modo que ela seja adequada aos alunos do 9° ano do Ensino Fundamental, pode-se utilizar funções afins do tipo $f(x) = ax + b$, $a \neq 0$ como chaves ao invés de matrizes inversíveis. Enfatiza-se que $a \neq 0$ garante a inversibilidade de uma função afim.

2.3.2. Adequação da cifra de Hill ao uso de funções

Para a execução do processo de ciframento e deciframento na cifra de Hill, utilizando uma função como chave, é essencial garantir que tal função seja inversível. Para tal, ela precisa ser bijetora. Alguns conceitos básicos acerca do conteúdo matemático a ser apresentado aos alunos do Ensino Básico para atividades envolvendo a cifra de Hill e funções são descritos a seguir e, posteriormente, será exibido. As definições matemáticas encontram-se de acordo com Iezzi e Murakami (2004).

Primeiramente, é importante a definição de função. Dados dois conjuntos A e B, não vazios, uma relação f de **A** em **B** recebe o nome de aplicação de A em B ou função definida em **A** com imagens em **B** se, e somente se, para todo $x \in A$ existe um só $y \in B$ tal que $(x, y) \in f$, isto é,

f é a aplicação de A em $B \Leftrightarrow (\forall x \in A, \exists \mid y \in B \mid (x, y) \in f)$.

Nesse caso, A é chamado de domínio de F, B de contradomínio de F e o subconjunto de B determinado por F é chamado de imagem de F. As notações utilizadas para se referir a tais denominações são $D(f)$, B, e $\Im(f)$, respectivamente.

Conforme características apresentadas, as funções podem ser classificadas de acordo com as seguintes proposições em:

· *Injetora:* A função $f : A \to B$ é injetora se, e somente se, quaisquer que sejam X_1 e X_2 pertencentes a de modo que $x_1 \neq x_2$ então $f(x_1) \neq f(x_2)$.

· *Sobrejetora:* A função $g : A \to B$ é sobrejetora se, e somente se, para todo pertencente a B existe um elemento pertencente a A tal que, $g(x) = y$. Nesse caso, a imagem e contradomínio de funções sobrejetoras são iguais.

· *Bijetora:* A função $f : A \to B$ é bijetora se,e somente se, F é sobrejetora e injetora.

Uma função admite inversa quando é bijetora. Tal resultado é garantido por teorema e pode ser consultado em Iezzi e Murakami (2004). Posto isso, a função bijetora F possui uma inversa dada por $f^{-1} : B \to A$, apresentando as seguintes propriedades:

(a) $D(f^{-1}) = B = \Im(f)$;

(b) $\Im(f^{-1}) = A = D(f)$;

(c) $(b, a) \in (f^{-1}) \Leftrightarrow (a, b) \in f$;

(d) o gráfico de (f^{1}) é simétrico do gráfico F de em relação a reta $Y = X$.

A fim de obter (f^{1}) da função inversível $f : A \to B$, definida pela lei $y = f(x)$, faz-se necessários os seguintes passos:

1. Primeiramente, $y = f(x)$ é transformada algebricamente de maneira que x seja expresso em função de y, ou seja, $x = F\text{-}1(y)$.

2. Depois, troca-se por e vice-versa, obtendo $\# = \# - 1(\#)$. A troca de x por y é dispensável, sendo recomendada apenas para facilitar a obtenção da função inversa. Aqui, vale destacar que pertence ao domínio de e $\#^{-1}$.

É possível provar que toda função afim do tipo $\# = \#\# + \#, \# \neq 0$ é bijetora e, consequentemente, inversível. Nesse caso, $\# = \#\# + \#, \# \neq 0$.

Com o objetivo de apresentar um exemplo da cifra de Hill, utilizando uma função afim como chave, considere que um grupo de soldados recebeu um bilhete de seu general com a mensagem: 78 – 358 – 58 – 62 – 2 – 74 – 2 – 22 – 358 – 18 – 54 – 78 – 18, e a chave $\#(\#) = 4\# - 2$.

Para decifrá-la, faz-se necessário a obtenção da inversa de #. Pelo que foi exibido anteriormente, $f^{-1}(x) = \frac{x+2}{4}$. Agora, basta substituir por cada valor numérico que compõe a mensagem, ou seja,

$f^{-1}(78) = \frac{78+2}{4} = 20,$

$f^{-1}(358) = \frac{358+2}{4} = 18,$

$f^{-1}(58) = \frac{58+2}{4} = 15,$

$f^{-1}(62) = \frac{62+2}{4} = 16,$

$f^{-1}(2) = \frac{2+2}{4} = 1,$

$f^{-1}(74) = \frac{74+2}{4} = 19,$

$f^{-1}(2) = \frac{2+2}{4} = 1,$

$f^{-1}(22) = \frac{22+2}{4} = 6,$

$f^{-1}(358) = \frac{358+2}{4} = 18,$

$f^{-1}(18) = \frac{18+2}{4} = 5,$

$f^{-1}(54) = \frac{54+2}{4} = 14,$

$f^{-1}(78) = \frac{78+2}{4} = 20,$

e $f^{-1}(18) = \frac{18+2}{4} = 5.$

Portanto, a mensagem decifrada é dada por: 20 – 18 – 15 – 16 – 1 – 19 – 1 – 6 – 18 – 5 – 14 – 20 – 5.

Convertendo a sequência de números obtidos em letras, de acordo com a correspondência exibida pelo Quadro 2, os soldados obtêm a mensagem tropas a frente.

Na próxima seção, o principal objetivo deste trabalho é concretizado por meio da proposição e exposição de uma oficina envolvendo a cifra de Hill e funções afins.

3. OFICINA PROPOSTA

Como já proferido ao longo desse artigo, pretende-se sugerir e mostrar que a criptografia pode ser introduzida na prática de ensino e aprendizagem de Matemática no Ensino Básico, por meio de uma oficina. Assume-se aqui que, ao associar o que está sendo estudado a algo concreto ou contextualizado, abram-se novas possibilidades de entendimento da disciplina. Neste sentido, Hinz (2000, p.23) afirma que "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 oficina foi inspirada pelo experimento denominado Mensagens Secretas com Matrizes, disponível no site https://m3.ime.unicamp.br/recursos/1123 da coleção Matemática Multimídia da Universidade Estadual de Campinas (UNICAMP). Contudo, ao invés de utilizar matrizes como conteúdo matemático, a mesma foi adaptada ao conteúdo de funções afins. A intenção de tal ajuste foi de que a oficina pudesse contemplar alunos do 9° ano do Ensino Fundamental. Além disso, a oficina foi implementada pela história da criptografia, com a finalidade de promover uma atitude de perscrutação nos estudantes, como é previsto na BNCC "[...] os estudantes devem desenvolver habilidades relativas aos processos de investigação, de construção de modelos e de resolução de problemas" (BRASIL, 2018, p.529).

No que se refere aos aspectos metodológicos, a oficina proposta foi organizada em três momentos, conforme descrito a seguir.

3.1. 1° Momento: abordagem histórica

Inicialmente, os alunos devem conhecer a história da criptografia, detalhes do seu uso em guerras e principalmente, o funcionamento da cifra de César. Sobre o último item, a sugestão é que seja proposto aos alunos um desafio como o exibido pela Figura 6, para que usando transposição, os mesmos possam chegar à mensagem matemática genial.

A cifra de César embasará o segundo momento da oficina. A ideia é que os estudantes entendam o funcionamento da transposição, como método que permite cifrar mensagens, sem a utilização de um conteúdo matemático específico.

OCVGOCVKEC IGPKCN

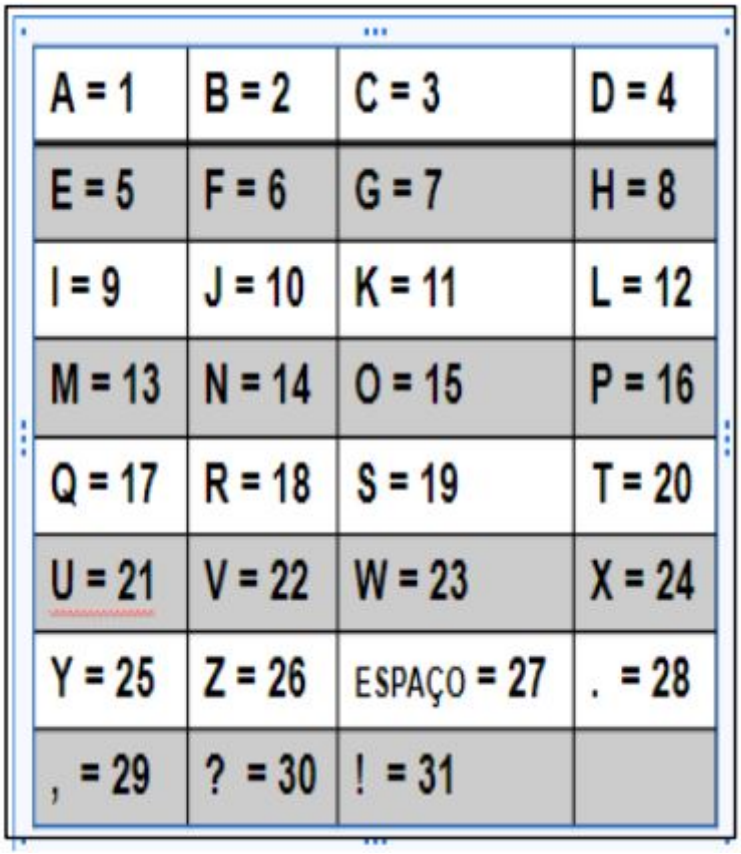
MATEMÁTICA GENIAL

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

FIGURA 6
Modelo de desafio envolvendo a cifra de Cesar
Fonte: Autoras

3.2. 2° Momento: exemplificação/ revisão do conteúdo

É interessante apresentar aos alunos uma tabela de pré-decodificação como a exibida pela Figura 7. Nela está o alfabeto e o número correspondente à cada letra. Destaca-se que a pré-codificação consiste na troca da letra pelo número equivalente.



A = 1	B = 2	C = 3	D = 4
E = 5	F = 6	G = 7	H = 8
I = 9	J = 10	K = 11	L = 12
M = 13	N = 14	O = 15	P = 16
Q = 17	R = 18	S = 19	T = 20
U = 21	V = 22	W = 23	X = 24
Y = 25	Z = 26	ESPAÇO = 27	. = 28
, = 29	? = 30	! = 31	

FIGURA 7
Tabela de pré-codificação
Fonte: Autoras

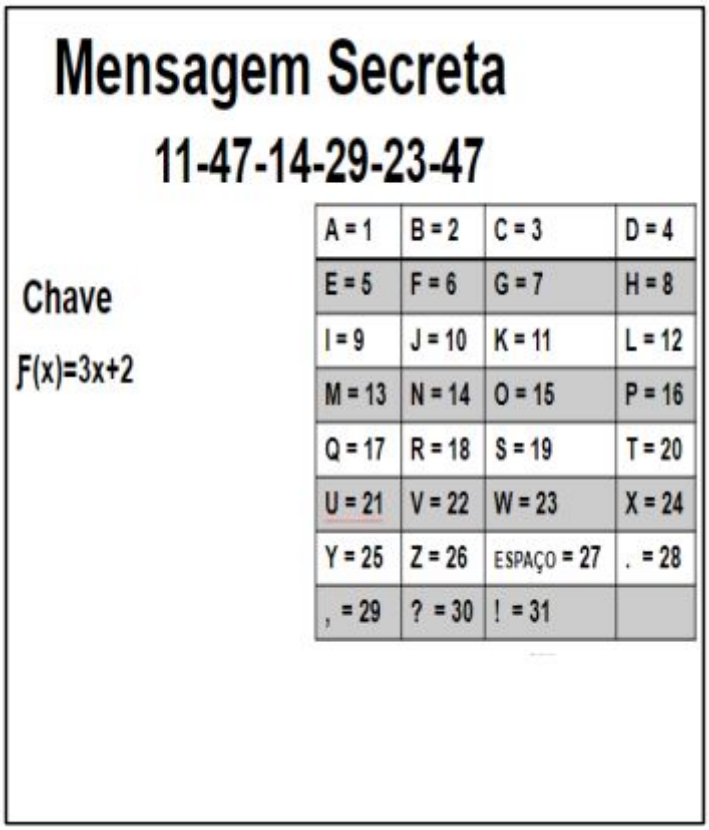


FIGURA 8
Mensagem para decodificação
Fonte: Autoras

Nesse momento, sugere-se a decodificação de uma mensagem secreta pelos alunos, utilizando a tabela de pré-codificação. Um exemplo é ilustrado na Figura 8. A priori, recomenda-se que os estudantes sejam orientados a desvendar/decifrar a mensagem secreta, sem nenhuma ajuda do professor. Esse instante pode ser aproveitado para instigar o interesse na atividade e não necessariamente, para que os alunos tenham sucesso.

É importante que o professor construa uma revisão conceitual, com a realização de exemplos, do conteúdo de funções e de como chegar a sua inversa, dando ênfase às funções afins, para que assim não haja dúvidas sobre o processo de cifragem e decifragem das mensagens que serão utilizadas na oficina. Após encerrar a parte da fundamentação, os alunos devem retornar à Figura 8, que contém a mensagem, a correspondência das letras do alfabeto com seus respectivos números e a chave que consiste em uma função afim. O esperado dos alunos, extraindo os dados da mensagem de decodificação, é que procedam como descrito a seguir.

A mensagem original foi codificada por meio da função $\#(\#) = 3\# + 2$. Para decodificar a mensagem secreta, é necessário que o recebedor calcule as imagens de $\# -1$, onde e $\#(\#) = \#(\# -1)$ e $\#(\# -1) = \#(\#)$. Para tal, encontra-se inicialmente . Nesse caso, conforme apresentado na Subseção 2.3, deve-se trocar **x** por y e vice-versa na função $\# -1\ (\#)$, obtendo $\# = 3\# + 2$. Posteriormente, isola-se a variável **Y**, chegando assim a a $\# -1$:

Utiliza-se $f^{-1}(x) = \frac{x-2}{3}$ para descriptografar a mensagem, calculando a imagem de cada número codificado, isto é, basta substituir os valores da sequência:

11 – 47 – 14 – 29 – 23 – 47

por *x,* Assim,

$f^{-1}(11) = \frac{11-2}{3} = 3$,

$f^{-1}(47) = \frac{11-2}{3} = 15,$
$f^{-1}(14) = \frac{14-2}{3} = 4,$
$f^{-1}(29) = \frac{29-2}{3} = 9,$
$f^{-1}(23) = \frac{23-2}{3} = 7,$
e $f^{-1}(47) = \frac{11-2}{3} = 15,$
obtendo-se a sequência:
3 – 15 – 4 – 9 – 7 – 15.

Agora, basta fazer uma substituição usando a Figura 8, alterando os números da sequência obtida pelas letras correspondentes, chegando à palavra código. Para que não reste dúvidas quanto ao processo criptográfico, faz-se necessário evidenciar aos alunos como o recado foi criptografado.

Destaca-se que a ação de cifrar uma mensagem, de acordo com o método utilizado, é um processo relativamente mais simples. A princípio, escolhe-se a mensagem, que no caso foi código, e em seguida, substitui-se cada letra pelo número correspondente, obtendo a seguinte mensagem pré-codificada:
3 – 15 – 4 – 9 – 7 – 15.

Substituindo os valores da sequência numérica obtida na função chave dada por $\#(\#) = 3\# + 2$, obtém-se a mensagem codificada. É relevante salientar aos alunos que essa função precisa ser invertível e, portanto, bijetora, frisando que, com exceção das funções constantes, toda função afim é inversível.

Codificando a mensagem, tem-se:
$\#(3) = 3 \cdot 3 + 2 = 11,$
$\#(15) = 3 \cdot 15 + 2 = 47,$
$\#(9) = 3 \cdot 9 + 2 = 29,$
$\#(7) = 3 \cdot 7 + 2 = 23,$
e $\#(15) = 3 \cdot 15 + 2 = 47,$
obtendo-se a mensagem $11 - 47 - 14 - 29 - 23 - 47$ que foi decodificada inicialmente.

3.3. 3° Momento: prática

Posteriormente ao segundo momento, a turma de alunos deverá ser dividida em grupos e cada grupo define uma mensagem a ser codificada. A sugestão é que cada grupo realize essa atividade com foco na tabela de pré-decodificação da Figura 7. Logo após criptografarem as mensagens escolhidas, estas devem ser trocadas aleatoriamente entre os grupos para serem descriptografadas, permitindo que toda a turma participe do processo de criptografar e descriptografar e tenha a oportunidade de exercitar cálculos envolvendo funções afins. Os estudantes podem definir novas chaves para suas mensagens, diferentes daquela exibida pela Figura 8, desde que estas sejam divulgadas ao grupo que decifrará a mensagem.

3.4. Avaliação da oficina

As oficinas, como já reforçado ao longo do artigo, são ferramentas que auxiliam a construção do conhecimento. Para Paviani e Fontana (2009, p. 78) caracterizam as oficinas pedagógicas como um sistema que para obter sucesso, deverá agregar teoria e prática:

> A articulação entre teoria e prática é sempre um desafio, não apenas na área da educação. Entre pensar e fazer algo, há uma grande distância que, no entanto, pode ser vencida. Um dos caminhos possíveis para a superação dessa situação é a construção de estratégias de integração entre pressupostos teóricos e práticas, o que, fundamentalmente, caracteriza as oficinas pedagógicas.

Além disso, as oficinas pedagógicas devem ser focadas na inclusão da diversidade apresentada pelos alunos de uma turma, a fim de favorecer suas singularidades. Dessa forma, é importante a avaliação de qualquer estratégia ou metodologia inovadora em sala de aula pelo professor e pela turma de alunos envolvidos. Assim, propõe-se que, além da avaliação e reflexão do professor acerca do desenvolvimento da oficina proposta neste artigo em uma sala de aula, o professor também efetue uma avaliação da oficina pelos alunos. Destaca-se que, quando os estudantes têm a abertura de conversar sobre as atividades propostas pelo professor, os mesmos podem acompanhar seus próprios desenvolvimentos e se envolverem efetivamente no processo de ensino e aprendizagem.

Tal avaliação pode ser realizada por meio de um questionário, por exemplo, na intenção de verificar se a turma assimilou os conhecimentos conforme foram colocados e de aperfeiçoar a oficina para seu desenvolvimento em uma outra turma. Nesse caso, um questionário pode ser utilizado para levantar sugestões, questionar os pontos de maior interesse, listar os pontos nos quais os alunos tiveram mais dificuldade e averiguar se a ferramenta de ensino foi útil para o aprendizado de funções afins. Algumas perguntas que poderiam compor tal questionário são sugeridas no Quadro 3.

QUADRO 3
Questões sugeridas

A oficina contribuiu para o seu conhecimento? A história do conteúdo apresentado favorece seu interesse pelas aulas de matemática? Você já tinha ouvido falar em criptografia? A oficina despertou seu interesse para se aprofundar no tema? A oficina colaborou com o seu cinhecimento acerca das funções afins? Sua concepção sobre o significado e funcionamnto da criptografia mudou ao final da oficina?Justifique.

Fonte: Autoras

4. CONSIDERAÇÕES FINAIS

Parte dos alunos do Ensino Básico não consegue desenvolver um raciocínio lógico matemático, muitas vezes por estarem expostos a um processo de ensino e aprendizagem de conteúdos não contextualizados. Neste artigo, parte-se do pressuposto de que a contextualização da Matemática no cotidiano do aluno não deve passar desapercebida tendo em vista sua potencialidade em dar valor à existência e à importância da Matemática.

Este pensamento converge à proposta da BNCC, documento normatizador das aprendizagens necessárias do Ensino Básico e suas devidas competências, de que a Matemática deve ser ensinada de forma que o estudante fosse letrado matematicamente, de modo que consiga interpretar, raciocinar e sugerir problemas em contextos diversos.

Neste sentido, a criptografia é considerada aqui com potencialidade em promover o letramento matemático e em despertar o interesse dos alunos pela disciplina de Matemática, tendo em vista sua contínua aplicabilidade no mundo contemporâneo e tecnológico. Assim, uma oficina foi proposta como estratégia de integração do conteúdo de função afim com a prática e cotidiano dos alunos do 9° ano por meio da criptografia.

A oficina visa a história como introdução, a fim de motivar os alunos com os porquês da criação de códigos e sua evolução conforme o desenvolvimento tecnológico, acreditando que a mesma possa fornecer uma base aos alunos para expandirem seus conhecimentos por meio de um aprofundamento em criptografia e nos conteúdos matemáticos que serão aplicados junto a ela.

Como continuidade deste trabalho, pretende-se desenvolver a atividade descrita neste artigo em uma turma do 9° ano do Ensino Fundamental, avaliá-la e identificar pontos que devem ser melhorados para devidas adaptações. Por fim, espera-se que este trabalho auxilie e inspire docentes em suas aulas, tendo em vista que a criptografia pode ser uma grande conciliadora entre teoria e realidade possibilitando o sucesso do ensino e aprendizagem de diversos conteúdos matemáticos.

REFERÊNCIAS

BORGES, Fábio. Criptografia como Ferramenta para o Ensino de Matemática. **Anais da SBMAC.** Pág, v. 822.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular.** Brasília, 2018.

COUTINHO, Severino. **Criptografia**. Rio de Janeiro. IMPA, 2015.

CUNHA, Rhuan Gonzaga da; SOUZA, Gláucio Barbosa de; PEREIRA, Eduardo Elias; SILVA, Vinicius Spneli Forzan. **Criptografia de dados utilizando matrizes.** Minas Gerais: Re3C, 09 nov. 2016. Disponível em: https://revistas.unifenas.br/index.php/RE3C/article/view/100 . Acesso em: 25 maio 2019.

GALDINO, Uelder Alves. **Teoria dos números e Criptografia com Aplicações Básicas** TESE (MESTRADO PROFISSIONAL-PROFMAT/CCT/UEPB) -PARA´IBA: UEPB, 2014, 77 p.

GROENWALD, Claudia Lisete Oliveira; OLGIN, Clarissa de Assis. **Códigos e senhas no ensino básico**. Disponível em: http://sbem.iuri0094.hospedagemdesites.ws/revista/index.php/EMR-RS/article/view/1463. Acesso em: 25 ago. 2021.

HINZ, Marco A. M. **Um estudo descritivo de novos algoritmos de criptografia.** Pelotas: UFP, 2000.

IEZZI, G.; MURAKAMI, C. **Fundamentos de matemática elementar 1**: conjuntos, funções. 8. ed. São Paulo: Atual, 2004.

MENEZES, Rosilene de. **Criptografia e Álgebra.** 2013. 66 f. TCC (Graduação) - Curso de Matemática, Universidade Federal de Minas Gerais, Belo Horizonte, 2003.

PAIXÃO, Jéssica Shayanne da. **Criptografia: história, atividades e divulgação científica.** Tese de Doutorado. Universidade de São Paulo, 2020.

PAVIANI, Neires; FONTANA, Niura. **Oficinas pedagógicas: relato de uma experiência.** CONJECTURA: filosofia e educação, v. 14, n. 2, 2009.

PEREIRA, Nádia Marques Ikeda. **Criptografia: uma nova proposta de ensino de matemática no ciclo básico.** 2015.

APÊNDICE 1

AGRADECIMENTOS

Não se aplica.

FINANCIAMENTO

Não houve financiamento

CONTRIBUIÇÕES DE AUTORIA

Resumo/Abstract/Resumen: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.
Introdução: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.
Referencial teórico: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.

Análise de dados: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.
Discussão dos resultados: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.
Conclusão e considerações finais: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.
Referências: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.
Revisão do manuscrito: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.
Aprovação da versão final publicada: Ariane Andressa Noronha de Sousa Miranda, Fernanda Vital de Paula.

CONFLITOS DE INTERESSE

Os autores declararam não haver nenhum conflito de interesse de ordem pessoal, comercial, acadêmico, político e financeiro referente a este manuscrito.

DISPONIBILIDADE DE DADOS DE PESQUISA

O conjunto de dados que da suporte aos resultados da pesquisa foi publicado no próprio artigo.

CONSENTIMENTO DE USO DE IMAGEM

Não se aplica.

APROVAÇÃO DE COMITÊ DE ÉTICA EM PESQUISA

Não se aplica.

COMO CITAR - ABNT

MIRANDA, Ariane. PAULA, Fernanda V. Expandindo os horizontes do ensino básico por meio da criptografia. **REAMEC – Rede Amazônica de Educação em Ciências e Matemática.** Cuiabá, v. 9, n., 2, e21059, maio a agosto, 2021. https://doi.org/10.26571/reamec.v9i2.12652

COMO CITAR - APA

Miranda, A. A. N.S., & Paula, F. V. (2021). Expandindo os horizontes do ensino básico por meio da criptografia. *REAMEC - Rede Amazônica de Educação em Ciências e Matemática,* 9(2), e21059. https://doi.org/10.26571/reamec.v9i2.12652

LICENÇA DE USO

DIREITOS AUTORAIS

PUBLISHER

Universidade Federal de Mato Grosso. Programa de Pós-graduação em Educação em Ciências e Matemática (PPGECEM) da Rede Amazônica de Educação em Ciências e Matemática (REAMEC). Publicação no Portal de Periódicos UFMT. As ideias expressadas neste artigo são de responsabilidade de seus autores, não representando, necessariamente, a opinião dos editores ou da referida universidade.

EDITOR

Dailson Evangelista Costa
Orcid: https://orcid.org/0000-0001-6068-7121
Lattes:http://lattes.cnpq.br/9559913886306408

Ligação alternative

https://periodicoscientificos.ufmt.br/ojs/index.php/reamec/article/view/12652 (pdf)