PEER REVIEW, Vol. 5, Nº 21, 2023
DOI: 10.53660/1128.prw2666
ISSN: 1541-1389

Ensino de matrizes na educação básica: uma experiência com criptografia

Teaching matrixes in basic education: an experience with cryptography

Jordan Gustavo da Silva
ORCID: https://orcid.org/0009-0002-4560-4994
Instituto Federal do Maranhão, Brasil
E-mail: jordan.gustavo90@gmail.com.
Arnaldo Silva Brito
ORCID: https://orcid.org/0000-0003-4162-2204
Univeridade estadual do Piauí, Brasil
E-mail: arnaldosilva@ccm.uespi.br
Rui Marques Carvalho
ORCID: https://orcid.org/0000-0003-2151-8733
Instituto Federal do Piauí, Brasil
E-mail: rui.marques@ifpi.edu.br
Sandoel de Brito Vieira
ORCID: https://orcid.org/0000-0002-5822-2111
Universidade Federal do Piauí, Brasil
E-mail: sandoelpi@gmail.com
Antonio Freitas Aguiar
ORCID: https://orcid.org/0000-0001-9760-8001
Instituto Federal do Piauí, Brasil
E-mail: antonioaguiar1805@gmail.com
Lucas Pereira Viana
ORCID: https://orcid.org/0009-0000-0763-5883
Instituto Federal do Maranhão, Brasil
E-mail: lucas.viana@ifma.edu.br
Raimundo Luna Neres
ORCID: https://orcid.org/0000-0001-9082-7885
Universidade Ceuma- UNICEUMA – São Luís/MA, Brasil
E-mail: raimundolunaneres@gmail.com

RESUMO

Neste trabalho aborda-se o ensino e aprendizagem de matrizes na Educação Básica, com o objetivo de proporcionar aos alunos, a partir desse objeto do conhecimento produzir aplicações práticas e contextualizá-las com resultados significativos, por meio de métodos e técnicas de criptografia utilizando as cifras de Hill. Trata-se de uma pesquisa qualitativa de intervenção, realizada com 29 alunos de uma escola pública Federal do município de Picos/Piauí/Brasil. Para isso, inicialmente, discutiu-se com os alunos a relevância do objeto de conhecimento no processo de aprendizagem. Em seguida, aplicamos as técnicas em estudo para construir um processo de codificação de mensagens, transmitidas abertamente, mas com controle do destinatário em relação às operações matriciais. A pesquisa revelou que, com aplicação da criptografia, os alunos demonstraram mais interesse pelo objeto de estudo e se apropriaram das interações ocorridas entre a teoria e a prática, levando-nos a concluir que houve aprendizagem.

Palavras-chave: Ensino de matrizes; Criptografia; Cifras de Hill; Educação Básica.

Recebido: 30/08/2023 | Aceito: 28/09/2023 | Publicado: 02/10/2023

ABSTRACT

This work deals with the teaching and learning of matrices in Basic Education, with the aim of providing students with practical applications from this object of knowledge and contextualizing them with significant results, through cryptographic methods and techniques using Hill ciphers. This is a qualitative intervention study carried out with 29 students from a federal public school in the municipality of Picos/Piauí/Brazil. To do this, we first discussed with the students the relevance of the object of knowledge in the learning process. We then applied the techniques under study to build a process of coding messages that were transmitted openly. However, the recipient had control over the matrix operations. The research revealed that, with the application of cryptography, the students showed more interest in the object of study and took ownership of the interactions that took place between theory and practice, leading us to conclude that learning had taken place.

Keywords: Teaching matrices; Cryptography; Hill ciphers; Basic Education.

INTRODUÇÃO

Neste artigo apresentamos uma discussão sobre o ensino e aprendizagem de matrizes utilizando como instrumento de ensinagem técnicas de criptografia por meio das cifras de Hill no processo de construção do conhecimento de alunos do terceiro ano do Ensino médio de uma escola pública do Estado do Piauí.

Durante anos de nossa atuação como professor de matemática, temos observado que o ensino de matemática está sempre passando por renovação. Renovação esta que, às vezes, não está relacionada somente a conteúdos, mas também aos objetivos e metodologias a serem abordados em cada novo objeto de conhecimento, nos diferentes níveis do ensino da educação básica.

Em nossas praxis professorais constatamos que a aprendizagem já não é observada como um simples processo de transmissão e recepção de informações, mas como uma construção de conhecimentos que se estimula com a investigação e observação dos alunos, traçando um paralelo entre teoria e realidade. Nossa investigação encontra amparo na teoria de PIAGET (1979), que ao observar o desenvolvimento de crianças, mostrou que o processo de desenvolvimento do conhecimento se dá por meio de interação entre sujeito e objeto. Por outro lado o,

> Construtivismo não é uma prática ou um método; não é uma técnica de ensino nem uma forma de aprendizagem; não é um projeto escolar; é, sim, uma teoria que permite (re)interpretar todas essas coisas, jogando-nos para dentro do movimento da história – das culturas, das sociedades, da humanidade e do universo. (BECKER, 2012, p.113).

Nessa pesquisa buscamos contextualizar o processo de ensino e aprendizagem de matemática promovendo uma educação inovadora e trabalhando a matemática com base no construtivismo, na qual o aluno possa traçar um caminho por meios próprios, com tentativas, erros e acertos. Em tese, uma abordagem em que a matemática seja vista e relacionada ao mundo real, com aplicações em situações do cotidiano, não como algo distante de sua realidade e sem utilidade.

Para responder esses questionamentos, trabalhamos, em forma de oficinas, durante um bimestre escolar, com duas turmas de terceiro ano do ensino médio. O objeto de conhecimento era matrizes usando criptografia por meio de cifras de Hill e mostrando sua importância e aplicação na matemática.

Nessa teia de raciocínio, inicialmente, apresentamos os conceitos básicos de criptografia, estabelecendo uma nova forma de enviar e receber mensagens para os discentes, de modo que poderiam ocultar mensagens em textos e símbolos visíveis a qualquer pessoa, ao passo que somente o destinatário original poderia descobrir o que aquele texto ou símbolo significava, processo completamente subsidiado pelo conteúdo de matrizes.

Vislumbramos que esse modelo de ensino, usando criptografia aplicada ao conteúdo de matrizes poderia responder de maneira satisfatória aos anseiso dos estudantes tanto em relação à aprendizagem desse objeto de conhecimento quanto às necessidades de contextualização.

Neste sentido, elegemos como objetivo da pesquisa propor uma nova abordagem para o ensino de matrizes no âmbito do ensino médio, de forma a proporcionar aos alunos a possibilidade de visualizar intervenções em situações práticas, a partir da aplicação do conteúdo de matrizes. Essa abordagem encontra amparo na Lei 9.394/1996 (Lei de Diretrizes e Bases da Educação Nacional - LDBEN) definida para o ensino de matemática na educaçao básica.

FUNDAMENTAÇÃO TEÓRICA

Temos observado no dia a dia da sala de aula que o aluno se apropria do conteúdo quando ele pode traçar relações entre suas experiências com o material didático. Entretanto, na maioria das vezes, temos dificuldade para ajustar o processo de ensino-aprendizagem, por priorizá-lo como uma mera forma de transmissão de conhecimentos matemáticos, na forma de meros algoritmos, isolados da realidade, deixando de possibilitar uma construção e desenvolvimento lógico no discente. Para que isso ocorra,

> É preciso que o conhecimento escolar se constitua no processo ativo de interlocução entre educandos e educadores, tomados na multiplicidade das dimensões cognitivas, afetivas, éticas e estéticas constitutivas do processo educativo que busca a construção de cidadãos ativos e emancipados. A educação emancipadora é foco da escola. Se a escola somente repassar conteúdos, ter sempre boas notas e resultados em avaliações e não preocupar-se em despertar o sentimento de mudança social nos seus educandos, assim como formá-lo político, cultural, antropológico e economicamente, essa escola não tem qualidade e não tem caráter emancipador (GÓIS. 2015. p. 33).

Acreditamos que mudar a forma como a matemática é vista por alguns estudanes, como sendo algo acessível somente para alunos especiais, é uma tarefa à qual os professores das matemáticas devem se dedicar para desmistificar esse jargão. E mostrar

a relevância da matemática no desenvolvimento do aluno, na condição de um ser social, como previsto nos Parâmetros Curriculares Nacionais pode ser ainda mais difícil,

> [...] a matemática pode dar sua contribuição à formação do cidadão ao desenvolver metodologias que enfatizem a construção de estratégias, a comprovação e justificativa de resultados, a criatividade, a iniciativa pessoal, o trabalho coletivo e a autonomia advinda da confiança na própria capacidade para enfrentar desafios (BRASIL, 1998, p. 27).

Admitimos que o docente de matemática não pode esquecer que esta disciplina, no ensino médio, tem um valor formativo essencial, pois ajuda a estruturar o pensamento, o raciocínio lógico e dedutivo, fundamental para a vida do estudante.

Somos de acordo que a matemática, hoje, não pode mais ser vista somente como uma ciência abstrata, mas sim como uma área de conhecimento com um papel bem definido, de formação de pensamentos e aquisição de habilidades, propiciando ao aluno o desenvolvimento de competências, técnicas e a capacidade de resolver problemas, investigar, analisar e enfrentar novas situações e desafios, ou seja, ser capaz de ter uma visão ampla da realidade.

Observamos, na escola pesquisada, que ainda existe, dentre alguns professores, hipóteses de que a matemática é uma disciplina feita somente para os alunos mais inteligentes, o que às vezes prejudica aqueles que não possuem o mesmo rítmo de aprendizagem, ademais.

> [...] quando o aluno possui afinidade com a matemática e o seu conteúdo, pouco interfere na aprendizagem a metodologia, o material didático utilizado e a forma como o professor conduz a aula, porém, cada aluno reage diferentemente, e estes fatores tornam-se significativos para aqueles que possuem dificuldades em aprender. (SOARES 2009 apud Abreu, Ferreira, 2014, p.4)

Constatamos em nossa região, ainda, uma predominância do ensino de matemática pelo método tradicional (em que só o professor é o mentor do conhecimento e o aluno um ser passivo), ou seja: pautado em aulas expositivas, baseadas apenas no uso do livro didático e do quadro, sem o auxílio de qualquer outro material didático. Em que os objetos de conhecimento, comumente, são desvinculados das situações cotidianas dos estudantes, gerando, assim, um distanciamento natural entre estes e o assunto a ser aprendido.

Observamos, também, que, de forma geral, o conteúdo de matrizes é tratado na sala de aula como um mero algoritmo de álgebra, suscetível de aplicações somente ao se

estudar a matemática mais avançada. Dessa forma, nossa pesquisa se justifica, dando outra abordagem e aplicação no ensino e aprendizagem de matrizes.

Buscamos o desenvolvimento ao propor uma interação entre o discente e o meio em que ele está inserido por meio de abordagens que propiciam uma contextualização do tópico de matrizes que seja acessível ao estudante da educação básica.

Nesse context, baseamos nossos estudos no método construtivista de ensino, uma vez que entendemos que tal modelo busca aproximação do discente ao objeto a ser compreendido por meio de estratégia que lhe permita compreender os temas estudados estando inseridos no meio em que vive. Com isso, é possível que ele possa se apropriar mais facilmente dos processos de ensino. A Teoria do construtuvismo,

> Propõe uma modalidade de aquisição do conhecimento em que o sujeito de modo ativo, compreenda cada fase do processo, perceba os nexos causais existentes entre eles e incorpore como seu aquele conteúdo e não que reconstrua por si mesmo a bagagem científica já constituída. Talvez se justifique o termo construtivismo como uma condenação ao processo impositivo de transmissão do conhecimento. Levanta a possibilidade de uma transmissão sem imposição e de uma recepção sem a característica da passividade (WERNECK. 2006. p. 180).

Com base nessa proposição, propomos o ensino usando abordagens que podem auxiliar ao docente no seu papel de facilitador da aprendizagem ao apresentar aos seus alunos(as) modelos que permitam a interação entre estudante e objeto a ser estudado em matrizes, ou seja: Criptografia e Cadeias de Markov, que permitem uma contextualização do estudo de matrizes, podendo, ainda, propiciar melhoria da compreensão mostrando onde podem ser utilizados nos dias atuais. O professor tem papel fundamental nesse processo de ensino e aprendizagem por meio de metodologia construtivista, entende-se que o professor deve adotar sempre uma postura diferenciada que busque os seguintes aspectos.

> primeiro: é importante para o professor tomar consciência do que faz ou pensa a respeito de sua prática pedagógica. Segundo, ter uma visão crítica das atividades e procedimentos na sala de aula e dos valores culturais de sua função docente. Terceiro, adotar uma postura de pesquisador e não apenas de transmissor. Quarto, ter um melhor conhecimento dos conteúdos escolares e das características de aprendizagem de seus alunos (MACEDO. 2010. p. 61)

Levantamos hipóteses de que com este trabalho possamos despertar em nossos colegas professores mais uma forma de desenvolver suas atividades de ensinagem, seja também uma fonte de inspiração e pesquisa. Haja vista que essa abordagem de ensino

utilizando métodos de criptografia por meio das Cifras de Hill pode aproximar o aluno do objeto de conhecimento que muitas vezes é tratado com distanciamento da realidade deles.

De acordo com ANTON e RORRES (2012) as cifras de Hill são sistemas poligráficos em que um texto é dividido em um conjunto de n letras, em que cada um destes conjuntos será substituído por n letras cifradas. Assim sendo, as cifras de Hill são baseadas em transformações matriciais.

No caso mais simples de cifra de Hill, abordado por ANTON e RORRES (2012) o texto será separado em grupos de duas letras, assim o procedimento a ser seguido é o seguinte:

Primeiro o texto da mensagem será substituído por um conjunto de símbolos numéricos e inseridos em uma matriz daí então multiplique-a pelas matrizes de codificação sendo está uma matriz invertível que satisfaça os critérios para multiplicação entre matrizes com a matriz gerada pela codificação da mensagem, por fim, converta a matriz da mensagem em uma nova matriz de valores numéricos que contém a mensagem criptografada.

A ideia básica da criptografia é que as informações sejam codificadas usando um esquema de criptografia e decodificadas por qualquer pessoa que conheça o esquema. Existem muitos esquemas de criptografia que variam de muito simples a muito complexos. A maioria deles é de natureza matemática. Neste trabalho, adotamos a cifra de Hill, em que o codificador é uma matriz e o decodificador a inversa dessa matriz codificadora.

Com a finalidade de explicitar modelo de execução de uma cifra de Hill, buscamos o trabalho de Silva (2020), que utiliza uma matriz A como sendo a matriz de codificação, B a matriz formada pelos caractéres que compõem a mensagem e C a matriz que contêm a mensagem criptografada (os tamanhos de A e B terão que ser compatíveis a multiplicação entre eles e determinarão o tamanho de C). Ou seja: $A \cdot B = C$, (1). Alguém tem C e conhece A e deseja recuperar B, na equação (1). Para isso multiplica-se ambos os lados da equação (1) por A^{-1}, e tem-se $B = A^{-1} \cdot C$.

CAMINHO METODOLÓGICO

Trabalhamos com 29 alunos de duas turmas de terceiro ano do ensino médio, no auditório da escola, local onde ocorreu a oficina sobre criptografia por meio de cifras de Hill.

Inicialmente, discorremos sobre a contextualização histórica da criptografia e sua importância, como por exemplo, a quebra de códigos de mensagens na segunda guerra mundial, retratado no filme "O jogo da imitação". Em seguida, apresentamos um conjunto de técnicas necessárias para a realização da codificação e decodificação de mensagens utilizando as cifras de Hill, dentre elas o uso de uma tabela que consiste em uma cifra que busca associar letras e símbolos a números, o uso de multiplicação de matrizes para a codificação das mensagens e, em seguida, os conceitos de congruência aritmética e matriz inversa para a decodificação das mensagens.

Feitas as apresentações preliminares acerca do tema, os professores presentes fizeram um exemplo de codificação e decodificação de uma mensagem para todos os alunos presentes. Em seguida, aleatoriamente, formamos 7 grupos, sendo 1 grupo com 5 alunos e os demais com 4 alunos. Esse quantitativo de alunos por grupo tornou-se necessário para que pudéssemos viabilizar uma maior participação de todos os membros do grupo na realização das atividades.

Como primeira atividade, apresentamos aos alunos uma caça ao tesouro dentro da escola de maneira que cada grupo receberia 3 pistas, criptografadas, para descobrir em qual local procurar os próximos passos para encontrar o tesouro proposto nesta caçada. Ao decodificar as 3 pistas e descobrir em qual local a caçada teria sequência, os alunos recebiam uma senha, também criptografada, para que pudessem ter acesso às próximas pistas que lhe seriam entregues naquele local pelo responsável do setor, que só entregaria as novas pistas ao receber a senha que lhe fora informada pelos professores previamente. Este processo se repetiria por 3 vezes, sendo que o terceiro conjunto de pistas e senha levariam os alunos ao tesouro procurado.

Buscando aumentar um maior envolvimento de todos, os grupos os professores criaram duas trilhas de pistas distintas a serem percorridas. Cada uma das trilhas levaria a setores distintos da escola e nenhum grupo saberia a qual trilha pertenceria e somente poderiam identificá-la ao decodificar as suas pistas.

SITUAÇÃO VIVENCIADA E ESTRATÉGIAS UTILIZADAS

Os 7 grupos formados foram identificados pelas letras A, B, C, D, E, F, e G, como forma de preservar as sua identidades. A escolha dos alunos para compor cada grupo foi realizada por sorteio, com a finalidade de garantir a imparcialidade na distribuição entre os alunos que apresentaram maior ou menor afinidade com a matemática.

A caça ao tesouro teve início com cada grupo escolhendo ao acaso entre as duas possíveis trilhas a serem percorridas, aqui denominadas por *alfa* e *beta*. Os grupos A, C e D escolheram a trilha *alfa*, os grupos B, E, F e G escolheram a trilha *beta*. As trilhas foram montadas na seguinte ordem: a trilha alfa teve a seguinte sequência de pistas (elaborar, mestres e local), essas três pistas indicavam a sala dos professores como próximo local de busca. As senhas que dariam acesso a novas pistas foram (pato, tatu. Galo ou vaca), cada grupo só recebia uma dessas senhas. No próximo nível, as pistas foram (leitura, silêncio e estudo) indicando a biblioteca como próximo local de busca e as senhas disponíveis para este nível foram (mesa, faca, lata ou mala), neste setor receberiam as últimas três pistas (segurança, proteção, entrada), que indicariam o local onde o tesouro estava escondido indicando assim a guarita dos vigilantes e as possíveis senhas (vereda, pijama, inseto ou maleta) para ter direito a receber o tesouro. A sequência de pistas da trilha *beta* foi dada por (central, regras, fiscal) indicando o controle acadêmico da escola, com senhas (gato, sapo, rato ou leoa). Para o próximo nível, as pistas foram (conselho, intervenção, notificação), indicando o setor pedagógico, com senhas (cama, gelo, cano ou cola) para requerer as últimas pistas. As últimas pistas desta trilha foram (zelo, higiene, organização), indicando o setor de limpeza como local em que estaria o tesouro, tendo como senhas (quadro, perola, picolé ou panela) para requerer o tesouro escondido.

O grupo D foi a primeira a concluir a caça ao tesouro, levando 40 minutos para alcançar todo o percurso. Nesta equipe pudemos notar uma divisão de trabalho entre os alunos de modo que as três pistas tivessem o seu processo de decodificação acontecendo simultaneamente, de modo que três alunos resolviam as operações matriciais e o quarto

ficava como suporte para fazer as conversões de símbolos para números manuseando a tabela de encriptação[1] e ainda dando suporte aritmético com uso de calculadora.

Após o primeiro grupo ter concluído a sua caçada ao tesouro, os professores solicitaram aos alunos a ele pertencentes que se dividissem para auxiliar os demais grupos. Entretanto, sem dizer-lhes quais eram as palavras, somente com o suporte de como proceder em cada uma das etapas.

O grupo F foi o segundo a realizar todo o percurso com sucesso, levando um tempo de 80 minutos. o mesmo foram solicitados para ajudar os demais colegas nos mesmos termos que foram repassados para os estudantes do grupo D. O grupo B foi o último a realizar todo o percurso, levando um total de 180 minutos.

E, para exemplicar a utilização da criptografia no estudo de matrizes, apresentamos uma atividade desenvolvida com os alunos. Dessa forma, para fins de codificações de mensagens, adotamos a seguinte tabela de codificação:

Tabela 1: Cifra de codificação de mensagens

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

Fonte: Silva (2020, p. 30)

Os símbolos (., !, # e @) adicionais serão utilizados para tornar mais fácil a interpretação das mensagens, além disso, # e @ serão utilizados para representar espaços em branco entre cada palavra ou no fim da frase. E, ainda, o espaço vazio para o número trinta será utilizado para fins de redefinição de um algarismo quando por meio da

[1] É uma tabela que mostra a associação de cada letra ou símbolo a um número natural.

multiplicação de matrizes viermos a obter um número superior a 30, utilizamos o conceito de congruência[2] tratado em aritmética dos restos.

Com base nessas informações, podemos realizar operações reais de criptografia utilizando apenas os conhecimentos prévios de matrizes. Como por exemplo, na codificação da mensagem EU ESTUDO MATEMÁTICA. utilizando a matriz de codificação[3] $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$, de acordo com a tabela 1, a frase ficaria cifrada na forma $5 - 21 - 29 - 5 - 19 - 20 - 21 - 4 - 15 - 29 - 13 - 1 - 20 - 5 - 13 - 1 - 20 - 9 - 3 - 1 - 27$. Pela cifra de Hill devemos tomar agrupamento de n letras de forma a tornar possível a multiplicação entre as matrizes codificadora e a matriz que contém a mensagem, deste modo como a matriz codificadora é de ordem 3×3 iremos tomar grupamentos de três símbolos. Assim teremos:

$$\begin{matrix} 5 & 5 & 21 & 29 & 20 & 1 & 3 \\ 21 & 19 & 4 & 13 & 5 & 20 & 1 \\ 29 & 20 & 15 & 1 & 13 & 9 & 27 \end{matrix}$$

A partir dessas informações, monta-se uma matriz com estes grupamentos e realiza-se o procedimento de codificação desta matriz ao multiplicá-la pela matriz codificadora pré-definida. Assim,

Seja $B = \begin{bmatrix} 5 & 5 & 21 & 29 & 20 & 1 & 3 \\ 21 & 19 & 4 & 13 & 5 & 20 & 1 \\ 29 & 20 & 15 & 1 & 13 & 9 & 27 \end{bmatrix}$ a matriz que contém a mensagem e A a matriz codificadora. Calculando o produto tem-se:

$$A \cdot B = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 5 & 5 & 21 & 29 & 20 & 1 & 3 \\ 21 & 19 & 4 & 13 & 5 & 20 & 1 \\ 29 & 20 & 15 & 1 & 13 & 9 & 27 \end{bmatrix}$$

$$= \begin{bmatrix} 134 & 103 & 74 & 58 & 69 & 68 & 86 \\ 137 & 99 & 64 & 17 & 57 & 56 & 109 \\ 29 & 20 & 15 & 1 & 13 & 9 & 27 \end{bmatrix}$$

[2] Definição: seja dado um número inteiro m maior do que 1. Diremos que dois números inteiros a e b são congruentes módulo m se a e b possuírem mesmo resto quando divididos por m. Neste caso, simbolizaremos esta situação como segue: $a \equiv b \; mod \; m$.

[3] A matriz de codificação deve ser obrigatoriamente uma matriz que admita inversa.

A matriz produto é a matriz codificada. Entretanto, percebemos que a maior parte dos números não está na tabela de símbolos pré-definidos. Neste caso, utilizamos congruência, $mod\ 30$, pois com esse procedimentos todos os seus restos se tornarão menores do que 30, isso serve para definir quais os seus equivalentes dentro da tabela de símbolos. Deste modo, temos:

$134 \equiv 14\ (mod\ 30)$

$137 \equiv 17\ (mod\ 30)$

$103 \equiv 13\ (mod\ 30)$

$99 \equiv 9\ (mod\ 30)$

$74 \equiv 14\ (mod\ 30)$

$64 \equiv 4\ (mod\ 30)$

$58 \equiv 28\ (mod\ 30)$

$69 \equiv 9\ (mod\ 30)$

$57 \equiv 27\ (mod\ 30)$

$68 \equiv 8\ (mod\ 30)$

$56 \equiv 26\ (mod\ 30)$

$86 \equiv 26\ (mod\ 30)$

$109 \equiv 19\ (mod\ 30)$

Dessa forma, a matriz codificada será equivalente a

$$\begin{bmatrix} 14 & 13 & 14 & 28 & 9 & 8 & 26 \\ 17 & 9 & 4 & 17 & 27 & 26 & 19 \\ 29 & 20 & 15 & 1 & 13 & 9 & 27 \end{bmatrix}$$

Por consequência, a mensagem criptografada seria escrita da seguinte maneira:

NQ#MITNDO!QAI.MHZIZS.

Ao receber a mensagem codificada o destinatário, conhecendo a chave de decodificação, pode obter a mensagem original simplesmente remontando a matriz, já conhecendo a quantidade de letras que compõem cada grupamento, e multiplicando-a pela inversa da matriz codificadora. Assim:

Se $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$ é a matriz codificadora da mensagem, ao calcularmos sua inversa, ~~então~~ obteremos a matriz $A^{-1} = \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}$ esta será a matriz que trará a mensagem original de volta ao fazer o seu produto pela matriz gerada pela mensagem codificada.

$$\begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 14 & 13 & 14 & 28 & 9 & 8 & 26 \\ 17 & 9 & 4 & 17 & 27 & 26 & 19 \\ 29 & 20 & 15 & 1 & 13 & 9 & 27 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 5 & 21 & 29 & 20 & 1 & 3 \\ 21 & 19 & 4 & 13 & 5 & 20 & 1 \\ 29 & 20 & 15 & 1 & 13 & 9 & 27 \end{bmatrix}$$

CONSIDERAÇÕES FINAIS

Com este estudo buscamos oportunizar novas estratégias de ensino e aprendizagem para trabalhar conexões entre o objeto de conhecimento matrizes e a realidade em que o estudante está inserido, apresentando ao professor e ao aluno novas pespectivas de ensinagem, ou seja: outra opção ao professor da Educação Básica de como desenvolver o ensino e aprendizagem de matrizes de maneira a aproximá-lo de situações que são capazes de envolver e empolgar o estudante no uso de conhecimentos matriciais.

Observamos ao longo da pesquisa uma efetiva participação dos alunos e uma evolução em relação ao desenvolvimento das operações matriciais, tais como: adição, subtração, multiplicação e inversa de matrizes.

Constatamos, também, que foi enorme o leque de possibilidades que se abriu a partir do método apresentado, haja vista que os alunos puderam usar a criptografia com o viés do lúdico, e ainda tendo a possibilidade de serem trabalhados em feiras culturais, gincanas escolares, jogos escolares e caças ao tesouro, como demonstrado anteriormente.

Destarte, a aplicação da Criptografia no ensino e aprendizagem de matrizes não deve ser vista como a solução do ensino de matrizes, e sim como mais uma ferramenta a ser utilizada na educação matemática.

Espera-se que esta pesquisa tenha fortalecido a aprendizagem dos alunos e contribuído com o conhecimento didático pedagógico dos professores dela participantes.

Em suma, a pesquisa revelou que todos os participantes se mostraram capazes de trabalhar, com habilidade, a utilização da criptografia em operações matriciais, o que lhes proporcionou o conhecimento de mais uma metodologia, até então, não conhecida por eles. No entanto, vale destacar que não se deve considerar que os problemas da educação serão resolvidos com a mobilização pelo aluno dessa metodologia de ensino. Encare-se, portanto, designar-se, como mais uma alternativa de ensino.

REFERÊNCIAS

ABREU, Carlos Eduardo de Paula; FERREIRA, Francinildo Nobre, **O ensino da matemática contextualizado**, disponível em https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=967&id2=245. Acesso em 20 abr. 2023.

ANTON, Howard; RORRES, Chris. **Álgebra Linear: com aplicações**. Tradução: Claus Ivo Doering. 10. ed. Porto Alegre: Anton Textbooks, Inc, 2012. 784 p. v. Único.

BECKER, F. ***Educação e construção do conhecimento***. [S.l.]: Penso, 2012.

BRASIL, **Parâmetros curriculares nacionais: Matemática: terceiro e quarto ciclos do ensino fundamental: introdução aos parâmetros curriculares nacionais**, Brasília: MEC/SEF, 1998

BRASIL, **Lei nº 9.394, de 20 de dezembro de 1996. Diretrizes e Bases da Educação Nacional**, Brasília, DF. 1996.

GÓIS, Débora dos Santos. **Contribuições do curso de extensão a distância formação continuada em Conselhos Escolares Fases I e II na formação do professor**. In: MARTINS, Cibelle Amorim; SILVA, Cátia Luzia liveira da; VASCONCELOS, Francisco Herbert de Lima (orgs.). Conselho escolar: fortalecendo redes para a gestão democrática. 1. ed. vol. 3. Fortaleza: Encaixe, 2015.

SILVA, Jordan Gustavo da. **Abordagens para contextualização no ensino de matrizes na educação básica.** 2020. 56 f. Dissertação(Profmat). Universidade estadual do Piauí. 2020.

MACEDO, L. de. **Ensaios Construtivista**. [S.l.]: Casa do Psicólogo, 2010.

PIAGET, J. **A construção do real na criança**. Trad. Álvaro Cabral. Rio de Janeiro: Zahar, 1970. 360p.

WERNECK, Vera Rudge. **Sobre o processo de construção do conhecimento: o papel do ensino e da pesquisa**. Ensaio: aval.pol.públ.Educ., Rio de Janeiro, v. 14, n. 51, p. 173- 196, jun/ 2006. Disponível em: <https://www.scielo.br/j/ensaio/a/yy5rBTwpxjnh4mq7QWcFDwN/?format=pdf&lang=pt>. Acesso em: 24 abr. 2023.