



CRİPTOGRAFIA E MATRIZES: INTERAÇÃO E APRENDIZAGEM NO PROCESSO DE CODIFICAÇÃO DE MENSAGENS

Jhonatas da Silva Nascimento¹
Wagner Ferreira de Santana²
Wagner Ferreira de Santana³

RESUMO

Durante o processo acadêmico, percebi que alguns alunos tinham dificuldade em relacionar a Matemática com outros conteúdos, principalmente com seu cotidiano. Mediante a essa indagação, comecei a buscar formas de sanar essas dificuldades, até que, por meio de uma proposta de ensino desenvolvido por uma aluna do curso de Matemática em sua defesa de TCC que tinha como objetivo trazer uma relação entre a Matemática e a criptografia, despertou-me o interesse em colocar em prática, e tentar proporcionar aos alunos um melhor desempenho quando relacionamos a Matemática com outros conteúdos. Para poder pôr em prática a pesquisa, solicitei ajuda do professor de Álgebra linear e começamos a analisar a proposta. Posteriormente, desenvolvemos planos de aula, nos quais apresentamos o conteúdo de Matrizes por meio da criptografia, que tem como objetivo a codificação que está atrelada às formas de comunicação, por exemplo, os aplicativos de mensagens, fato que é muito vivenciado no cotidiano.

Palavras-chave: Aprendizagem; Matrizes; Criptografia.

INTRODUÇÃO

Com o decorrer do curso de Licenciatura em Matemática na UNEB Campus/VII Senhor do Bonfim BA, principalmente, quando cursava a disciplina de Matemática III surgiu o interesse de como poder relacionar o assunto de Matrizes com o cotidiano dos alunos, propondo aulas mais dinâmicas que fizessem com que os discentes tivessem mais vontade de aprender.

¹ Graduando do Curso de Licenciatura em Matemática da Universidade do Estado da Bahia-UNEB, jhonatas.mat28@gmail.com;

² Mestre do curso de Matemática da Universidade Federal do Vale do São Francisco-UNIVASF/IMPA, wfsantana@uneb.com;

³ Professor Orientador: Mestre, Universidade Federal do Vale do São Francisco-UNIVASF/IMPA, wfsantana@uneb.com;



Durante a minha trajetória no curso, especificamente nas disciplinas de estágio, percebia uma grande dificuldade dos alunos em compreender os assuntos matemáticos. Com isso, percebi que se conseguisse relacionar o conteúdo com algumas vivências do dia a dia dos alunos, poderia facilitar o entendimento, mas até o momento não tinha ideia de como poderia realizá-lo.

Ao assistir à defesa de monografia da aluna do curso de Licenciatura em Matemática da UNEB/Campus VII, que tinha como tema (A Cifra de Hill como Aplicação de Matrizes), despertou em mim a curiosidade em saber se a proposta demonstrada pela discente que relacionava Matrizes com Criptografia, poderia de fato, trazer resultados satisfatórios. A partir desse momento, solicitei a ajuda do professor de álgebra Linear e assim passamos a pesquisar e traçar uma maneira de colocar em prática o que foi salientado naquele trabalho, pois a proposta apresentada pela aluna era muito interessante e se encaixava no que queríamos.

O trabalho tem como objetivo desenvolver a proposta apresentada anteriormente na defesa de TCC e perceber como os discentes reagiriam ao ensino de Matrizes, sendo abordado a partir da criptografia, relacionado ao seu cotidiano.

Apesar da técnica de codificação de mensagens não ser tão difundida, queremos evidenciar que a Criptografia está no dia a dia dos educandos, como no caso de aplicativos de mensagens, e que a mesma tem relação com a Matemática.

A partir do que foi salientado anteriormente, averiguaremos o quanto isso pode instigar o interesse dos alunos no conteúdo de Matrizes e também o quanto os ajudará no processo de aprendizagem, que é de extrema importância para que possamos ter parâmetros que nortearão nossa pesquisa e assim, poder de fato, elucidar a ideia que, o ensino da Matemática pode ser algo mais prazeroso e que os alunos podem obter mais interesse pela disciplina quando associarem suas vivências diárias com a mesma.

Entendemos que essa pesquisa é de grande valia, pois faz com que os alunos percebam a relação entre a Matemática e suas vivências diárias, como no caso da criptografia que utiliza o conteúdo de Matrizes e está ligado a algo que eles utilizam bastante que são os aplicativos de mensagens. É por esse caminho que queremos mostrar que a Matemática está mais perto dos alunos do que eles imaginam e que temos que desfrutar desses conhecimentos para que



futuramente possamos desenvolver estudos e consolidar a ideia de que a Matemática faz parte de nossas vidas.

Além do que foi citado anteriormente, poderemos contribuir para que os discentes disponham de um processo de aprendizagem diferenciado, possibilitando que aprendam Matemática de forma mais dinâmica e entendendo que a mesma dispõe de aplicabilidade, pois era notório na fala dos discentes, no meu processo de estágio, que a Matemática é um conhecimento que se restringe somente à sala de aula e que depois não terá mais nenhum contato com o que tinham aprendido.

Esse é um dos pensamentos que pode ser mudado, pois sabemos que a Matemática se relaciona com outras disciplinas e que ela está presente em nosso dia a dia, e é mostrando isso para os alunos que tentaríamos mudar suas formas de pensar em relação à Matemática.

METODOLOGIA

Para iniciarmos o nosso objetivo, iremos utilizar uma pesquisa de cunho qualitativo, haja vista que queremos perceber como se dará o processo de aprendizagem, através da participação nas aulas e desenvolvimento das atividades.

Optamos, então, por um estudo de caso que parte da investigação e análise de dados onde segundo Yin (2005, p. 32), “o estudo de caso é um estudo empírico que investiga um fenômeno atual dentro do seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidas”. Ressaltando a ideia de que é necessário analisar e conhecer os fatos para que se obtenha resultados precisos.

A priori, foi selecionada uma turma do terceiro ano do Ensino Médio do Colégio Polivalente na cidade de Miguel Calmon-BA, com 15 alunos. Apresentamos o projeto ao professor de Matemática da turma, que ao entender do que se tratava, cedeu algumas aulas para a realização do mesmo. A opção de escolher uma turma do Ensino Médio deve-se ao fato de que é nessa etapa que se aborda o conteúdo em questão e esta turma especificamente já tinha estudado o conteúdo de Matrizes, assim facilitaria o desenvolvimento do projeto, pois os alunos poderiam fazer uma comparação em relação as duas formas que foram apresentadas o conteúdo.



Era necessário iniciar os estudos expondo sobre a Criptografia, questionando se algum deles teria conhecimento desse assunto, ou se já ouviram falar. Depois, para poder ter uma maior interação com os discentes e também proporcionar para os mesmos uma relação com o seu cotidiano mostramos uma forma muito fácil deles perceberem essa experiência.

Foi solicitado que pegassem os celulares, e os que tivessem acesso a algum aplicativo de mensagens, que nos dias atuais se tornou um dos grandes meios de comunicação, principalmente entre os jovens, que iniciassem uma nova conversa. Quando realizadas essas etapas, aparece uma imagem, apresentando a informação de que as conversas feitas serão criptografadas de ponta a ponta, isso quer dizer, que tudo que for conversado será codificado para que, caso haja alguma interceptação, não se saiba o teor da conversa. Nesse momento, houve uma grande interação entre os alunos, eles passaram a perceber o conteúdo de forma diferenciada, pois foi uma surpresa para eles saber que a Criptografia está em algo que eles tanto utilizam.

Logo após, já tendo uma noção do que é Criptografia e de como o conteúdo está presente no nosso cotidiano, foi explicado como a mesma pode ser colocada em prática, citando como exemplo a cifra de Cesar que é uma das mais simples formas de codificação. Ela é formada por meio do alfabeto onde cada letra é substituída por outra como está ilustrado na imagem abaixo.

A	M	C	D	E	F	G	O	I	R
Z	P	Q	W	Y	U	T	V	B	H

Um exemplo dado foi a palavra AMOR que codificada ficou ZPVH. Mostramos que para decodificar, existe uma relação inversa e passamos a realizar atividades em sala de aula, nas quais foi pedido para codificar palavras como, por exemplo, os seus nomes, e que outros alunos decodificassem palavras para identificar a mensagem original. Nesse momento, o entusiasmo tomou conta da sala, eles se sentiam muito empolgados em poder realizar aquela atividade e em descobrir aquele novo conhecimento, foi ai que passamos a falar que existem outros métodos de codificação, dentre eles a Cifra de Hill, e que para tal utilizaríamos algumas operações com Matrizes.



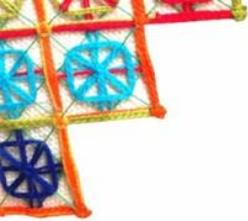
Em seguida, foram sanadas algumas dúvidas que surgiram e realizamos algumas atividades para reforçar o entendimento do conteúdo. Passamos a relembrar as operações com Matrizes, principalmente, a multiplicação de Matrizes, sempre salientando aos alunos que ao final do conteúdo iremos juntar o conteúdo de Matrizes com a Criptografia, para que os mesmos criem a curiosidade em saber como será essa mescla entre os dois conteúdos e foi assim, que os alunos se mantiveram concentrados, pois para eles era algo diferente poder unir a Matemática com algo que tinham tanto contato como as redes sociais.

Depois da explicação, foi realizada uma atividade com as operações com Matrizes para reforçar o entendimento dos alunos. Nessas atividades tinham; adição, subtração e multiplicação de Matrizes. Após responder a atividade junto com os mesmos, continuamos o conteúdo de criptografia, falando um pouco sobre a cifra de Hill, que por meio de técnicas, algumas delas já citadas anteriormente, é possível fazer o processo de codificação e o seu inverso através de números e letras, tornado assim, as mensagens mais protegidas.

Na cifra de Hill, ele utiliza as letras do alfabeto que são enumeradas, assim já formando um processo de codificação. Depois disso, são formadas com os números as mensagens que foram codificadas. Logo após, se utiliza uma Matriz para ser a CHAVE, que terá como objetivo proteger ainda mais as informações. Essa Matriz será multiplicada pela Matriz formada pelos números que foram utilizados a partir do alfabeto. Com isso, surgirá uma nova Matriz que terá novos valores e formarão novas letras que serão substituídas de volta no alfabeto. Nesse projeto, não utilizaremos todas as técnicas usadas na cifra de Hill, mas essas servirão como base para o trabalho.

Mediante os conteúdos que foram explanados para os alunos, foi realizada uma atividade em que a turma foi dividida em 2 grupos. Foi exposta uma palavra no quadro e o primeiro grupo teve o objetivo de codificá-la. Prosseguindo, o segundo grupo ficou responsável por decodificá-la. Logo após propor essa atividade, percebemos que a turma estava muito empolgada em querer realizar a atividade.

Assim, ao final da atividade foi entregue aos alunos um questionário para que os mesmos expressassem sua opinião de como foi a experiência de aprender o conteúdo de Matrizes da maneira que foi abordada, lembrando que os discentes já tinham tido contato com o conteúdo de Matrizes anteriormente.



No questionário trouxemos as seguintes perguntas: Você gostou de saber que a Matemática está ligada às redes sociais? Entendeu o que é Criptografia e para que serve? O que chamou sua atenção nas aulas? Teve alguma dificuldade com o assunto que estava sendo abordado? Foi mais fácil compreender o assunto de Matrizes por meio da Criptografia? A partir das perguntas elencadas, juntamente com as demais propostas desenvolvidas no decorrer do projeto, pudemos analisar se a utilização de atividades envolvendo suas vivências cotidianas trariam melhorias para o desempenho dos discentes.

FUNDAMENTAÇÃO TEÓRICA

Para ter um melhor entendimento dos conteúdos estudados, faz-se necessário conhecermos a definição de Matrizes e Determinantes. “Chamamos de Matriz uma tabela de elementos dispostos em linhas e colunas”. (BOLDRINI, 1980, p.1)

Observe a estrutura geral de uma matriz.

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} = [a_{ij}]_{m \times n}$$

“Quando nos referimos ao determinante, isto é, ao número associado a uma Matriz quadrada $A = [a_{ij}]$ como seção anterior, escrevemos: $\det A$ ou $[A]$ ou $\det [a_{ij}]$ ”. (BOLDRINI, 1980, p.66)

De forma geral, o determinante de uma matriz é dado pela seguinte definição: $\det[a_{ij}] = \sum_{\rho} (-1)^J a_{1j_1} a_{2j_2} \dots a_{nj_n}$, onde $J = J(j_1, \dots, j_n)$ é o número de inversões da permutação (j_1, \dots, j_n) e ρ indica que a soma é estendida a todas as $n!$ permutações de $(1, 2, \dots, n)$.

Um conteúdo que também é necessário para que haja melhor desempenho do conteúdo é a multiplicação de Matrizes.

“Se A for uma matriz $m \times r$ e B uma matriz $r \times n$, então o produto AB é a matriz $m \times n$ cujas entradas são determinadas como segue. Para obter a entrada na linha i e coluna j de AB , destacamos a linha i de A e a coluna j de B . Multiplicamos as entradas correspondentes da linha e da coluna e então somamos os produtos resultantes”. (ANTON, 2012, p.44)



Por meio dessa definição, teremos mais embasamento para transmitir para os alunos o conteúdo e poder proporcionar aos mesmos um material de qualidade.

Outro conteúdo que é necessário ter um maior entendimento é Criptografia. Houaiss (2007) afirma que a palavra Criptografia vem do grego *kriptos*, que significa secreto, e *graphia* que significa escrita.

Segundo Houaiss, (2007)

“Conjunto de princípios e técnicas empr. Para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; [...] em operações políticas, diplomáticas, militares, criminais etc., modificação codificada de um texto, de forma a impedir sua compreensão pelos que não conhecem seus caracteres ou convenções”.

Segundo Fiarresga (2010),

Um dos registros mais antigos de Criptografia aconteceu há 4000 anos, numa vila chamada Menet Khufu, no Egito antigo, no túmulo de Khnumhotep II, o arquiteto do faraó Amanemhet II. Ele construiu alguns monumentos para o faraó, as quais precisavam ser documentados.

Porém, estas informações escritas em tabletes de argila, não poderiam cair no domínio público. O arquiteto teve a ideia de substituir algumas palavras ou trechos do texto. Assim, caso o documento fosse roubado, o tesouro permaneceria protegido e o ladrão morreria de fome, perdido nas catacumbas da pirâmide.

Segundo os Parâmetros Curriculares Nacionais do Ensino Médio, um dos objetivos da Matemática no Ensino Médio é “aplicar seus conhecimentos matemáticos a situações diversas, utilizando-os na interpretação da ciência, na atividade tecnológica e nas atividades cotidianas” (PCN, 1997, p. 42). Podemos assim, observar que a utilização de meios que sejam facilitadores para o ensino da Matemática faz com que os alunos tenham a oportunidade de descobrir novas formas de compreenderem o assunto. E é por meio dessas práticas de ensino que o projeto visa a ajudar ainda mais no desenvolvimento no processo de aprendizagem da Matemática.

Há muito tempo, existe a preocupação com o ensino de Matemática e a sua significação para o aluno.

Segundo, D'AMBROSIO, 1989 salienta:

Em nenhum momento no processo escolar, numa aula de matemática geram-se situações em que o aluno deva ser criativo, ou onde o aluno esteja motivado a



solucionar um problema pela curiosidade criada pela situação em si ou pelo próprio desafio do problema. Na matemática escolar o aluno não vivencia situações de investigação, exploração e descobrimento. O processo de pesquisa matemática é reservado a poucos indivíduos que assumem a matemática como seu objeto de pesquisa. É esse processo de pesquisa que permite e incentiva a criatividade ao se trabalhar situações com problemas.

Foi nesse sentido que buscamos fazer essa pesquisa, e agora traremos os resultados de todo o trabalho, seja durante os momentos das atividades, como dos questionários respondidos.

RESULTADOS E DISCUSSÃO

A partir das atividades propostas, bem como na exposição dos conteúdos apresentados, pude observar que houve uma participação dos alunos nas atividades e uma interação com os colegas, assim a curiosidade dos discentes foi aumentando, despertando neles a vontade de saber cada vez mais sobre o conteúdo que seria abordado.

Um dos momentos que chamaram bastante minha atenção, foi quando apresentei a primeira possibilidade de codificação, através da Cifra de César, o momento de codificarem seus nomes e outras palavras quaisquer, os alunos demonstraram muito interesse e percebi que todos começaram a participar da atividade. Na decodificação, os discentes ficaram alvoroçados com a possibilidade de descobrirem uma mensagem e começaram a interagir entre os colegas, enviando mensagens codificadas para que o outro pudesse decodificar.

Em outro momento, comecei a revisar os conteúdos sobre Matrizes, os educandos ficaram curiosos quanto ao modo da utilização das matrizes no processo de codificação, haja visto que mencionei a necessidade do mesmo. Então, notei que o nível de interesse dos alunos era maior do que numa aula onde não há expectativa de aplicação do conteúdo, pois eles mesmos relataram que a utilização da criptografia tornou o conteúdo mais interessante, logo eles teriam a possibilidade de observar que a Matemática pode se relacionar com outros conteúdos. Isso ratifica o que D'Ambrosio afirma em seu texto que a curiosidade do aluno em pesquisar, descobrir, interagir, deve estar presente na aula de Matemática, para que a mesma faça sentido para o aluno.

Ao final, com as informações obtidas no questionário, pude elucidar ainda mais o objetivo em descobrir se a utilização de um conteúdo complementar poderia tornar a aprendizagem da disciplina de Matemática mais interessante. Pude observar que na primeira pergunta em que foi questionado se eles gostaram de saber que a Matemática está ligada às



redes sociais, todos os alunos falaram que sim e se mostraram bastante interessados em querer saber mais sobre o que poderia ser abordado em sala de aula.

Já na segunda pergunta, queria saber se os discentes entenderam o que é Criptografia e para que serve. As respostas foram bem concisas, pois relataram que conseguiram entender sua função, mas em alguns casos houve um pouco de dificuldade em relatar a sua relação com a Matemática. Percebi então, que isso ocorre pelo fato de os alunos sempre terem entendido a Matemática como uma disciplina que tem como objetivo o aprendizado escolar e não conseguirem relacionar a mesma com o seu dia a dia.

A terceira pergunta foi feita com intuito de descobrir o que chamou mais a atenção deles nas aulas. Os alunos responderam que nesse momento foi possível entender que a Matemática está relacionada com as redes sociais, porque não faziam a menor ideia que isso era possível e que agora olhariam com mais atenção para a disciplina e ressaltaram que dessa forma foi mais interessante aprender.

Dando continuidade à atividade, a quarta pergunta tinha como finalidade saber se eles tiveram alguma dificuldade com o assunto que estava sendo abordado, e a maioria deles disseram que conseguiram compreender, sendo que no decorrer das aulas, principalmente a parte que envolvia os cálculos matemáticos eram as que eles mais erravam. Então, pude perceber que uma grande parte dos discentes sabiam como realizar o desenvolvimento do cálculo, mas se atrapalhavam em realizá-lo. Foi aí que os ajudei com dicas e assim os alunos conseguiram realizar as atividades que eram propostas. Com isso, eles se sentiram realizados e empolgados para realizar novas atividades, o que era muito gratificante, pois podia perceber que os alunos estavam cada vez mais dispostos a aprender.

Finalizando o questionário, em relação a quinta pergunta que consistia em avaliar se foi mais fácil compreender o assunto de Matrizes por meio da Criptografia, os alunos afirmaram que sim, foi realmente uma experiência muito gratificante e as descobertas ao decorrer das aulas era a parte mais interessante, pois despertava neles a curiosidade em querer descobrir como seriam as novas propostas de ver a Matemática e mais ainda em saber que a mesma está relacionada com o cotidiano.

Diante das respostas obtidas no questionário, pude perceber que de fato o intuito da pesquisa estava sendo elucidada, pois no início das aulas, era percebido uma certa desmotivação



dos alunos ao se falar em Matemática, eles relatavam que isso não era para eles e que não gostavam, pois os mesmos pensavam que aprenderiam Matemática só na escola e que nunca mais iriam utilizar aquele conhecimento.

CONSIDERAÇÕES FINAIS

Diante de todos os dados dispostos no questionário das atividades e observações que foram realizadas em sala, pude perceber juntamente com o meu orientador, que de fato a utilização da Criptografia junto com a Matemática fez com que o processo de aprendizagem fosse mais produtivo, pois os alunos sentiram-se mais capazes de aprender os conteúdos com mais empenho.

Era notório o interesse que demonstravam em querer saber mais sobre o que estava sendo abordado e ainda mais em saber que a Matemática se relaciona com suas vivências do cotidiano, isso fez com que as aulas fluíssem de maneira bem agradável. Era de grande valia saber que os alunos estavam tendo a oportunidade de descobrir uma Matemática diferente com novas perspectivas em que a utilização da mesma no seu dia a dia era possível e agora eles poderiam ter mais empatia pela disciplina e ter a possibilidade de desmistificar a ideia de que ela é ruim e sem utilidades posteriores.

Constatamos que os discentes estiveram o tempo todo empolgados em saber cada vez mais, tanto mediante as perguntas como dando exemplos deles mesmos de como a Matemática está presente nas suas vidas como: no desconto quando iam comprar algo em uma loja à vista, saber qual será a média deles em uma determinada disciplina, a divisão da turma para fazer trabalho em grupo, e foi assim, que eles relataram que nunca tinham percebido essas situações de forma tão clara e que agora iam tentar perceber cada vez mais onde a Matemática poderia estar em suas vivências diárias

Essa pesquisa também foi de grande valia para nós, pois nela foi possível observar a importância na busca de formas diferenciadas de ensino, logo sua proposta possui grande relevância para fazer com que os alunos tenham a possibilidade de desmistificar a ideia que a Matemática é uma disciplina sem aplicabilidade, fazendo assim com que os mesmos possam desenvolver cada vez mais habilidades com a disciplina, e então, poder aprender mais sobre a Matemática que foi mostrada no decorrer da pesquisa, a qual traz possibilidades com descobertas e aprendizagens diversas.



O mais gratificante em poder realizar essa pesquisa foi poder proporcionar para os alunos novas ideias sobre a Matemática, pois eles conseguiram entender a proposta e que agora os alunos iriam propugnar a ideia que a Matemática é importante para o desenvolvimento do mundo e que se olharmos com mais atenção para as coisas que estão ao nosso redor, iremos perceber que a Matemática pode estar presente nelas e que isso nos possibilitará ter um maior entendimento da importância que a mesma desempenha na sociedade e em nossas vidas.

REFERÊNCIAS

ANTON, Howard; BUSBY, Robert C. Livro: **Álgebra linear contemporânea**, 1 ed.

ANTON, Howard; RORRES, Cris. Livro: **Álgebra linear com aplicações**, 10 ed.

BOLDRINI, José Luiz. Livro: **Álgebra linear**. São Paulo: Harper & How do Brasil, 1980.

D'AMBROSIO, Beatriz S. Como ensinar matemática hoje? **Temas e Debates**. SBEM. Ano II. N2. Brasília. 1989. P. 15-19.

Estudo de caso: **planejamento e métodos** / Robert K.

Yin [https://saudeglobaldotorg1.files.wordpress.com/2014/02/yin-](https://saudeglobaldotorg1.files.wordpress.com/2014/02/yin-metodologia_da_pesquisa_estudo_de_caso_yin.pdf)

[metodologia_da_pesquisa_estudo_de_caso_yin.pdf](https://saudeglobaldotorg1.files.wordpress.com/2014/02/yin-metodologia_da_pesquisa_estudo_de_caso_yin.pdf) >. Acesso 27 de mar de 2020.

FERREIRA, Sandra **A cifra de hill como aplicação de matrizes**, Universidade do Estado da Bahia, Faculdade Licenciatura em Matemática, 2015. Acessado em 28 agosto 2018.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática**. Universidade de Lisboa, Faculdade de Ciências, Departamento de Matemática, 2010.

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa**. Rio de Janeiro, Ed. Objetiva, 2007.

PCN. **Ciências da Natureza, 1997**. Página 42. Disponível em:

<<http://portal.mec.gov.br/seb/arquivos/pdf/ciencian.pdf>>. Acesso em: 03 de Jan. de 2020.