UNIVERSIDADE ESTADUAL DA REGIÃO TOCANTINA DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS, NATURAIS E TECNOLÓGICAS
LICENCIATURA PLENA EM MATEMÁTICA
NÍVEL GRADUAÇÃO

EMERSSON SILVA DA LUZ

MIZIA SILVA LIMA

CRIPTOGRAFIA: UMA ABORDAGEM PEDAGÓGICA PARA O ESTUDO DE MATRIZES NO ENSINO MÉDIO

IMPERATRIZ
2024

EMERSSON SILVA DA LUZ

MIZIA SILVA LIMA

CRIPTOGRAFIA: UMA ABORDAGEM PEDAGÓGICA PARA O ESTUDO DE MATRIZES NO ENSINO MÉDIO

Monografia apresentada ao curso Licenciatura em Matemática do Centro de Ciências Exatas, Naturais e Tecnológicas, da Universidade Estadual da Região Tocantina do Maranhão, como requisito para a obtenção do grau de Licenciado em Matemática.

Orientador:
Prof. Dr. Murilo Barros Alves

Imperatriz
2024

L979c

Luz, Emersson Silva da

Criptografia: uma abordagem pedagógica para o estudo de matrizes no ensino médio. / Emersson Silva da Luz; Mizia Silva Lima. – Imperatriz, MA, 2024.

74 f.; il.

Trabalho de Conclusão de Curso (Licenciatura em Matemática) – Universidade Estadual da Região Tocantina do Maranhão – UEMASUL, Imperatriz, MA, 2024.

1. Ensino de matemática. 2. Pedagogia - criptografia. 3. Matemática - matrizes. 4.Imperatriz - MA. I. Título.

CDU 511.82

Ficha elaborada pelo Bibliotecário: **Mateus de Araújo Souza CRB13/955**

Universidade Estadual da Região Tocantina do Maranhão – UEMASUL

Centro de Ciências Exatas, Naturais e Tecnológicas – **CCENT**

Trabalho de Conclusão de Curso de Licenciatura em Matemática: **Criptografia: Uma Abordagem Pedagógica para o Estudo de Matrizes no Ensino Médio**, de autoria de **Emersson Silva da Luz e Mizia Silva Lima**, aprovada pela banca examinadora constituída pelos seguintes professores:

Aprovada em 07/03/2024

Prof. Dr. Murilo Barros Alves – Orientador

Doutor em Engenharia de Produção e Sistemas

Prof. Dr. José Milton Lopes Pinheiro

Doutor em Educação Matemática

Prof. Me. Guimarães Vieira da Silva

Mestre em Matemática

AGRADECIMENTOS

Primeiramente a Deus, por ser o autor da vida e fortaleza maior durante toda essa longa jornada.

Ao grande orientador, professor e Doutor Murilo Barros Alves, cuja orientação sábia e apoio contínuo foram fundamentais para o desenvolvimento deste estudo. Sua dedicação e expertise foram pilares fundamentais para o sucesso deste trabalho.

A(o) amiga(o) e companheira(o) de trabalho pela parceria e incentivo incansável.

Gratidão imensa aos pais, familiares e amigos, cujo apoio incondicional e encorajamento foram a força motriz por trás de toda jornada acadêmica. Palavras de incentivo, compreensão e todo apoio necessário nos momentos de desafio, foram verdadeiramente inspiradores.

Ao grande amigo Roberto Viana de Sales, por seu incansável e constante apoio em tudo o que estava ao seu alcance.

A diretora pedagógica Aureni; aos professores Gardenia e Celsio e aos alunos do segundo ano do Ensino Médio do Colégio Militar Tiradentes II pela oportunidade, por todo apoio necessário e pelos valiosos *insights* e sugestões que forneceram ao longo do processo de pesquisa. Suas contribuições foram essenciais para a melhoria deste trabalho.

A todos os professores da graduação pela parceria, correções e ensinamentos ao longo de toda essa jornada acadêmica, pois todos tiveram sua parcela importante de contribuição no processo de evolução acadêmica e profissional desses formandos. Por fim, gratidão a todas as pessoas cujo trabalho acadêmico e literário contribuíram para a construção do referencial teórico deste trabalho.

Este projeto não teria sido possível sem o apoio e contribuição de cada um de vocês. Obrigado(a) por fazerem parte desta jornada.

Os autores, Mízia e Emersson.

RESUMO

Este trabalho propõe uma abordagem inovadora para o ensino de matrizes no Ensino Médio, integrando a criptografia como ferramenta pedagógica. Tal iniciativa se deu através da problemática sobre os barreiras enfrentadas por discentes e docentes no decurso da troca de conhecimento em relação ao tema matemático das matrizes. O dito assunto, normalmente é lecionado sem instigar a perspicácia e a motivação do aluno, resultando em *déficts* de aprendizagem. Cabendo considerar ainda, que em parcela dos contextos, os docentes o fazem dessa forma resumida, em decorrência da pouca oferta de tecnologia e possibilidades de trabalho. Nessa proposta, a cifra de Hill foi selecionada como meio para explorar os conceitos matriciais em um contexto prático e relevante para os alunos, onde o objetivo principal é oferecer uma estratégia que estimule o interesse dos estudantes pela Matemática, destacando sua aplicação na segurança da informação. Tendo em vista galgar a meta maior, desafios foram traçados e alcançados. Inicialmente, foi realizado um levantamento bibliográfico sobre a história da criptografia, sua importância para a segurança da informação e sua relação com a Matemática. Posteriormente, foram revisados conceitos básicos de matrizes que se relacionam com sua aplicação na criptografia. Os dados levantados, foram apresentados em uma palestra para docentes e discentes do Ensino Médio, visando fomentar a curiosidade dos mesmos a respeito dessa proposta pedagógica. Logo depois, os ouvintes foram levados para o Laboratório de informática da UEMASUL para uma atividade prática envolvendo o conteúdo de matrizes aplicado em criptografia com o auxílio do Software GeoGebra. Ao findar esse processo, todo o trabalho foi avaliado por meio de questionários e seus resultados apresentados por meio de relatos e gráficos estatísticos inovadores e de fácil compreensão. A apuração geral dos *feedbacks* que foram coletados através de questionários, resultaram na elaboração de gráficos estatísticos chamados de nuvem de palavras. Esses, por sua vez, fornecem *insights* sobre o impacto da abordagem pedagógica na compreensão e satisfação dos alunos. Diante dos resultados obtidos, cabe considerar que este estudo contribui para o avanço das estratégias de ensino de Matemática uma vez que, demonstra que a criptografia pode ser uma ferramenta poderosa para engajar os estudantes e promover uma compreensão mais profunda dos conceitos matriciais.

Palavras-chave: Criptografia. Hill. Matrizes. Pedagogia. Geogebra. Ensino Médio.

ABSTRACT

This paper proposes an innovative approach to teaching matrices in High School, integrating cryptography as a pedagogical tool. This initiative took place through problematic about the barriers faced by students and teachers during the exchange of knowledge regarding the mathematical topic of matrices. Such subject is normally taught without instilling student insight and motivation, resulting in learning deficits. It is also worth considering that in some contexts, teachers do so briefly. in short, due to the limited supply of technology and work possibilities. In this proposal, the Hill cipher was selected as a way to explore the matrix concepts in a practical and relevant context for students, where the main objective is to offer a strategy that stimulates students' interest in Mathematics, highlighting its application in information security. In order to reach the greater goal, challenges were outlined and achieved. Initially, a bibliographic survey was carried out on the history of cryptography, its importance for information security and its relationship with Mathematics. Subsequently, basic concepts of matrices that relate to its application in cryptography. The data collected was presented in a lecture for teachers and high school students, aiming to encourage their curiosity about this pedagogical proposal. Soon after, the listeners were taken to the Laboratory of UEMASUL for a practical activity involving the content of matrices applied in cryptography with the help of Software GeoGebra. By the end of this process, the entire work was evaluated through questionnaires and its results presented through innovative and easy-to-understand statistical reports and graphs. The general assessment of the feedback that was collected through questionnaires resulted in in the creation of statistical graphs called word clouds. These, in turn, provide insights into the impact of the pedagogical approach on student' understanding and satisfaction. Given the result obtained, it is worth considering that this study contributes to the advancement of Mathematics teaching strategies since it demonstrates that cryptography can be a powerful tool for engaging students and promoting a deeper understanding of matrix concepts

Keywords: Cryptography. Hill. Matrices. Pedagogy. Geogebra. High School.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização e problema de pesquisa

A criptografia é uma técnica utilizada para tornar informações sensíveis ilegíveis para indivíduos que não estão autorizados a ter acesso ao conteúdo dessas informações. É uma importante área da Ciência da Computação e desempenha um papel fundamental na segurança da informação em diversos contextos, como comunicações online, transações financeiras, armazenamento de dados, entre outros. No contexto educacional, a criptografia se apresenta como uma ferramenta que proporciona a contextualização de conteúdos matemáticos e promove uma melhor compreensão dos assuntos, além de contribuir para o despertar do interesse dos estudantes por questões relacionadas à tecnologia que é tão presente na vida cotidiana deles.

Este trabalho procura propor uma abordagem pedagógica para o ensino de matrizes por meio do contexto da criptografia. Por intermédio dessa proposta, busca-se entender como a criptografia pode ser utilizada como uma ferramenta pedagógica eficaz para ensinar conceitos de matrizes no Ensino Médio assim como promover uma forma de ensino que seja dinâmica e envolvente, de forma que desperte o interesse dos alunos pelo conteúdo, tornando-o mais atrativo através de uma contextualização que traga os conceitos matemáticos ensinados na sala para um campo mais prático.

Por ser um assunto considerado abstrato e muitas vezes estudado somente teoricamente, isto é sem muitas contextualizações, o campo de estudo das matrizes foi escolhido como foco desta pesquisa. Este viés matemático tem importância considerável na Matemática Aplicada, principalmente no meio computacional, mas que na sala de aula é frequentemente apresentado de forma pouco interessante. Espera-se por meio desta proposta fornecer aos alunos uma compreensão matricial mais sólida através de atividades práticas que tem por objetivo fomentar o interesse dos alunos.

No capítulo 2, alguns conceitos preliminares, começando com uma revisão da literatura sobre fatos históricos importantes da criptografia, seguido da fundamentação matemática necessária para a sua realização, onde serão comentados alguns conceitos de matrizes, operações com matrizes e conceitos de aritmética modular, além do detalhamento da Cifra de Hill que será o ponto principal da proposta pedagógica desta pesquisa. Ainda no capítulo 2 será

comentado a respeito do uso de softwares no ensino da matemática e como estes podem ser utilizados no estudo de criptografia. O capítulo será finalizado com a apresentação do software GeoGebra como ferramenta pedagógica.

No capítulo 3 serão apresentados os procedimentos metodológicos que virão a serem executados para a realização do trabalho. Será exposta a classificação desta pesquisa e detalhado o método de trabalho utilizado para desenvolver a proposta, como se deu a conscientização do problema, qual a sugestão, o detalhamento do desenvolvimento, a avaliação da pesquisa e a apresentação dos resultados.

No capítulo 4 serão apresentados e discutidos os resultados da pesquisa onde acontecerá o relato da sequência didática que aconteceu em dois momentos: uma palestra e um momento prático no laboratório de informática. Os resultados da palestra e da aula no laboratório serão discutidos através da análise de nuvens de palavras geradas a partir da respostas dos alunos a questionários referentes aos eventos. Além da nuvem de palavras será realizada uma análise de sentimentos ao final do capítulo 4. No capítulo 5, serão feitas as considerações finais referentes a esta pesquisa.

2 CONCEITOS PRELIMINARES

2.1 A criptografia ao longo do tempo

Já há muito tempo as pessoas procuram formas de comunicar-se. O processo de comunicação inclui o compartilhamento de informações, ensinamentos, ideias, mensagens, pensamentos, entre outros. Menezes (1973) considera que o desenvolvimento da comunicação foi fundamental para o surgimento da vida em sociedade e, em suas primeiras aparições, se manifestou em uma forma de linguagem simples que, com o tempo, foi apresentando formas melhores e mais evoluídas, o que facilitou a troca de informações entre as pessoas. Com a necessidade do desenvolvimento da economia e da sociedade, a comunicação passa por um processo de evolução com o surgimento da escrita, o que permitiu que as informações e conhecimentos fossem acessíveis e passados a um número cada vez maior de pessoas.

Morais e Noronha (2014) ressaltam que o advento da escrita contribuiu para o surgimento da necessidade humana de guardar segredos, sejam eles segredos pessoais, sentimentais, militares, religiosos ou governamentais. Isso favoreceu o compartilhamento de mensagens secretas, ou seja, mensagens que somente o emissor e o receptor podem decifrar. A partir daí, ao mesmo tempo em que a espécie humana adquiriu a capacidade de guardar segredos de determinados assuntos em mensagens escritas, surge também o desejo de decifrar essas mensagens. Assim, ao longo dos anos foram travadas batalhas entre aqueles que guardam segredos e aqueles que estão interessados nessas informações secretas e buscam desvendar essas mensagens. Nesse contexto, nasce a criptografia que tem por base a escrita de mensagens a partir de códigos secretos.

Criptografia (do Grego: kryptós, "oculto"+ graph de graphein, "escrever"), para Quaresma e Lopes (????), consiste em codificar mensagens confidenciais, com o intuito de proteger os dados da mensagem de terceiros pois está diretamente relacionada com a comunicação segura e tem sido uma ferramenta importante para a segurança de mensagens privadas. Ela envolve a transformação de informações em um formato ilegível, chamado de "texto cifrado"por meio de algoritmos matemáticos e chaves, de modo que somente as pessoas ou sistemas com a chave correta possam decifrar e compreender as informações originais.

Entre as principais fases de seu desenvolvimento encontra-se o período da criptografia clássica, que remete à sua origem e está relacionada às formas de criptografia que foram

desenvolvidas antes do surgimento da computação moderna e das técnicas criptográficas avançadas utilizadas atualmente. Os métodos utilizados eram baseados em princípios matemáticos e técnicas manuais para cifrar e decifrar informações. Segundo Almeida e Napp (2012) , a criptografia pode ter se originado no mesmo período do surgimento da escrita. Não é possível detalhar sobre a sua origem e muito pouco se sabe a respeito de suas primeiras aplicações. Em seu trabalho, Fiarresga et al. (2010) relatou que o registro mais antigo de criptografia é do túmulo de um nobre do Antigo Egito, Khnumhotep II, datado de cerca de 4000 anos atrás.

A criptografia esteve presente desde o sistema de escrita hieroglífica dos egípcios e foi muito utilizada na Antiguidade para codificar mensagens secretas trocadas durante as guerras com o objetivo de compartilhar planos de batalha. Um exemplo muito famoso dos primeiros modos de criptografar mensagens para esse fim, segundo Groenwald e Olgin (2010), é a Cifra de César. O processo de codificação da mensagem consistia em substituir cada letra da palavra pela letra que se encontrava em um determinado número de posições à frente no alfabeto.

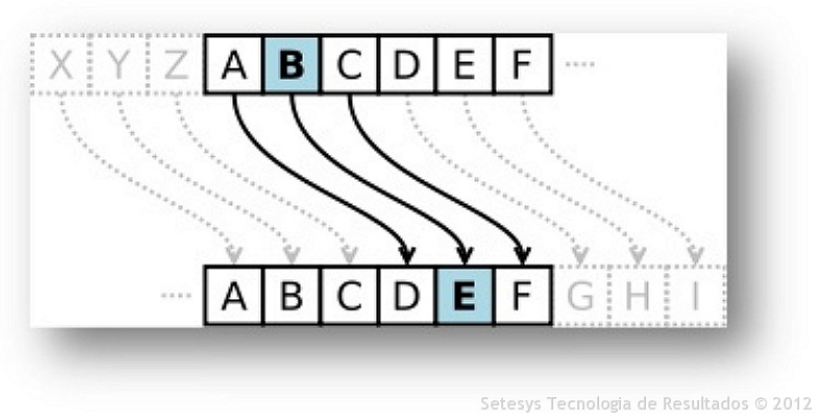

Figura 1: Cifra de César
Fonte: Google images (2023)

Por exemplo, utilizando o alfabeto latino e o português como idioma no qual a mensagem foi escrita, podemos codificar a palavra MATEMÁTICA utilizando a Cifra de César transformando cada letra na letra que está três posições à frente no alfabeto. Assim, a mensagem enviada seria PDWHPDWLFD. De acordo com Jesus Brito e Litoldo (2016), uma vez que a Cifra de César utiliza apenas um único alfabeto no processo de cifração de mensagens, pode ser classificada como sendo uma cifra monoalfabética, no entanto, esse era um método muito fácil de ser quebrado e, portanto, não apresentava muita segurança para o conteúdo da mensagem.

Como alternativa para a falta de segurança no método utilizado pela Cifra de César, surge, então, uma extensão dessa cifra que ficou conhecida como Cifra de Vigenère, sendo uma cifra polialfabética por ter em sua composição 26 alfabetos (Figura 2) e, que em vez de usar um único deslocamento para todas as letras, utiliza uma palavra-chave para determinar os deslocamentos individuais de cada letra do texto original. Consistia em dispor várias Cifras de César em sequência, formando uma tabela de alfabetos onde cada alfabeto estaria deslocado ciclicamente do anterior por uma posição. (JESUS BRITO; LITOLDO, 2016)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	F	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figura 2: Qaudrado de Vigenère
Fonte: Os Autores (2023)

Porto et al. (2015) narra em seu trabalho que para cifrar a mensagem utilizando a Cifra de Vigenère, era escolhida uma palavra-chave que seria repetida várias vezes até que tivesse o comprimento da mensagem que se desejava cifrar. Por exemplo, para cifrar a mensagem INIMIGOADIREITA com 15 letras, escolhendo como palavra-chave a palavra BOMB, com 4 letras, seria necessário repeti-la até atingir o comprimento do texto a ser cifrado e teria-se a mensagem BOMBBOMBBOMBBOM.

Texto	I	N	I	M	I	G	O	A	D	I	R	E	I	T	A
Chave	B	O	M	B	B	O	M	B	B	O	M	B	B	O	M
Cifra															

Figura 3: Mensagem e texto pré-cifrado
Fonte: Os Autores (2023)

Logo após concluir essa etapa do processo, faria-se uma combinação na tabela da letra

da mensagem original com a sua correspondente no texto pré-cifrado no qual utilizou-se a palavra-chave e então teria-se a mensagem cifrada. Utilizando o exemplo acima citado e a tabela, a letra I da mensagem original combinada com a letra B (primeira letra da mensagem pré-cifrada com o uso da palavra-chave) geraria a letra J que seria a primeira letra do texto cifrado, da mesma forma a letra N combinada com a letra O geraria a letra B, como mostrado na imagem abaixo. Fazendo o mesmo processo com o resto da mensagem, obteria-se o texto cifrado JBUNJUABEWBFJHM.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	F	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figura 4: Exemplo de codificação utilizando a Cifra de Vigenère
Fonte: Os Autores (2023)

Texto	I	N	I	M	I	G	O	A	D	I	R	E	I	T	A
Chave	B	O	M	B	B	O	M	B	B	O	M	B	B	O	M
Cifra	J	B	U	N	J	U	A	B	E	W	B	F	J	H	M

Figura 5: Mensagem, texto pré-cifrado e texto cifrado
Fonte: Os Autores (2023)

A Cifra de Vigenère é, de fato, mais segura que a Cifra de César tradicional, no entanto, a cifra de Vigenère também pode ser quebrada, especialmente se a palavra-chave for adivinhada ou se o texto cifrado for longo o suficiente para análise estatística. Por conta disso, Charles Babbage conseguiu desenvolver um método de decriptação para essa técnica o que fez com que os estudos em criptografia precisassem ser intensificados para que houvesse uma cifra mais segura como alternativa para a Cifra de Vigenère. Alguns anos depois nasceram outras variações da Cifra de César e a partir daí, iniciou-se um processo histórico milenar

em que diversos estudiosos deixaram suas contribuições para o aprimoramento de técnicas de codificação, tornando os métodos cada vez menos vulneráveis. (JESUS BRITO; LITOLDO, 2016)

Ao longo dos anos, com a evolução da tecnologia tornou–se necessário o aumento da complexidade nos métodos criptográficos. Percebe-se, então, que apenas as habilidades humanas naturais já não eram suficientes para criar sistemas de criptografias mais complexos, daí surge o uso de máquinas para auxiliar no processo de criptografia de mensagens. Silva et al. (2019) cita em seu trabalho que a máquina de cifra mais conhecida de todos os tempos é a máquina Enigma utilizada pelo exército alemão, durante a Segunda Guerra Mundial e, que revolucionou o mundo da criptografia.

Utilizada pelos nazistas, a máquina Enigma surgiu entre as duas guerras com o objetivo de codificar e decodificar mensagens compartilhadas entre o exército alemão durante a guerra. Ela realizava substituições bem mais complexas do que aquelas que eram, até então, humanamente possíveis de se fazer, embora fosse de funcionamento simples, suas engrenagens geravam milhares de possibilidades, o que tornava humanamente impossível decifrar sua mensagem. Entretanto, uma equipe de especialistas de diversas áreas, dos quais pode-se destacar Alan Turing, reunidos pelo governo britânico conseguiram desvendar os códigos alemães e puderam ter acesso ao conteúdo das mensagens cifradas pela Alemanha. (FIARRESGA et al., 2010)

Figura 6: Máquina Enigma
Fonte: https://pt.wikipedia.org/wiki/Enigma$_{\%}28m\%C3\%A1quina\%29$

Com o advento dos computadores e da internet, as pessoas vivem constantemente procurando ou compartilhando informações online, como em transações financeiras e conversas privadas. Com isso, dados pessoais estão sendo armazenados em algum lugar e muitas vezes não é possível ter certeza se esses dados estão sendo armazenados de forma segura ou não. Por isso, a segurança de dados tornou-se uma das principais preocupações da atualidade, o que resultou em métodos criptográficos cada vez mais avançados.

Ao longo dos anos, com a evolução da tecnologia, tornou–se necessário o aumento da complexidade nos métodos criptográficos. De acordo com Fiarresga et al. (2010), até meados da década de 70 todos os métodos já utilizados para criptografar mensagens eram simétricos, ou seja, até então com o mesmo algoritmo com o qual a mensagem era cifrada era possível decifrá - la. Por exemplo, utilizando a Cifra de César para codificar uma mensagem, o algoritmo de encriptação é um inteiro k ao mesmo tempo em que a chave de descriptografia é o inteiro -k, daí a necessidade de se manter a chave em sigilo. Denomina - se criptografia por chave simétrica, aquela em que a chave (o método de encriptação) deveria ser mantida em segredo, apenas o emissor e o receptor da mensagem poderiam ter acesso. Dessa forma, quem cifrasse a mensagem poderia decifrá-la e, consequentemente, o canal para a transmissão dessa chave precisava ser seguro. Também conhecido como criptografia por chave privada, sua segurança encontrava-se comprometida caso a chave de encriptação das mensagens fosse descoberta. Foi então que iniciaram - se estudos de métodos que possibilitassem o uso de duas chaves, surgindo, assim, o método assimétrico que possui uma chave pública e uma privada.

A fim de não precisar atribuir uma mesma chave ao emissor e ao receptor da mensagem, o método de criptografia por chave pública permite que cada indivíduo tenha sua chave pública que possibilita a encriptação de qualquer mensagem que alguém queira lhe enviar, de forma que somente sua chave privada será capaz de descriptografar a mensagem uma vez criptografada por sua chave pública. Em seu trabalho, Silveira e Faleiros (2005) compartilharam que na criptografia assimétrica, o individuo que receberá a mensagem mantém em público a chave que será utilizada para cifrar a mensagem e, em privado a que será utilizada para decifrar a mensagem, dessa forma, apenas o receptor da mensagem pode decifrá-la pois somente ele possui a chave que será utilizada no processo de descriptografia da mensagem.

Atualmente o método de criptografia assimétrica mais utilizado é o RSA, assim chamado porque leva as iniciais dos seus criadores R. L. Rivest, A. Shamir e L. Adleman. Consiste na escolha de dois números primos muito grandes, denominados de p e q, pelo emissário da mensagem. Após a escolha desses números define-se o valor de n que será o produto de p e

q ($n = pq$). O valor de n será denominado módulo. Também será definido um outro valor e que deve ser um número primo com $\phi(n)$ (o valor da Função de Euler que, quando n possui apenas dois fatores primos diferentes, no caso p e q, é $\phi(n) = (p-1)(q-1)$). Assim, o par de números (n, e) forma a chave pública, esses números serão usados pelo remetente para codificar a mensagem. O remetente terá a mensagem cifrada C calculando o resto da divisão de b^e por n, sendo b a mensagem original. Após receber a mensagem cifrada, o destinatário então poderá decifrar a mensagem C calculando o resto da divisão de C^d por n, sendo d o inverso de e em $\phi(n)$. A tripla (p, q, d) forma a chave privada que deverá ser mantida em segredo.

Segundo Andrade e Santos Silva (2012) a segurança oferecida pelo sistema RSA se baseia na dificuldade de fatorar um número inteiro que seja muito grande, pois ainda não existe um método totalmente eficaz para números com uma quantidade muito grande de algarismos. Para Barbosa et al. (2003), atualmente, o algoritmo mais eficiente é o método General Number Field Sieve, que conseguiu fatorar um número com 129 dígitos e para isso levou oito meses utilizando uma rede de 1600 computadores. É realmente muito demorado o processo de fatoração de um número primo tão grande, assim sendo, o método RSA se torna muito difícil de ser quebrado.

Em seu trabalho, Barreto et al. (2013) alega que em 1997, Peter Shor, um matemático estadunidense, descobriu um algoritmo quântico qualificado para fatorar números inteiros muito grandes em um curto período de tempo, o que causa novas preocupações para a segurança de técnicas convencionais de criptografia assimétrica, como é o caso do RSA. Isso significa que uma mensagem criptografada nos dias de hoje não necessariamente estará protegida em um futuro onde os computadores quânticos se tornem amplamente utilizados. Por isso a necessidade de fomento em pesquisas na área de criptografia assimétrica pós-quântica.

2.2 Fundamentação Matemática

Esta seção apresenta requisitos básicos de Matrizes e também de Teoria dos Números, especificamente sobre a *aritmética de resíduos módulo m*, necessários para uma compreensão matemática da Cifra de Hill que será detalhada adiante na seção 2.3.

2.2.1 Matrizes

As Matrizes são um tópico fundamental na matemática ensinada no ensino médio, sobretudo em álgebra linear. São importantes, principalmente, por sua aplicação em várias áreas, como física, estatística, ciências da computação, economia e engenharia. Nesta seção, será realizada uma revisão da álgebra elementar de matrizes. Para tanto, os conceitos apresentados foram coletados e uniformizados a partir de três referências, são elas: Anton e Busby (2006), Boldrini et al. (1980) e Lipschutz e Lipson (2011).

2.2.1.1 Notação Matricial e Terminologia

Chama-se *matriz* uma tabela de elementos dispostos em linhas e colunas. Por exemplo, ao recolher-se os dados referentes as notas de três alunos nas disciplinas de Português, Matemática e Física pode-se dispô-las na seguinte tabela:

Notas dos alunos 1, 2 e 3			
Disciplina	Aluno 1	Aluno 2	Aluno 3
Português	7,5	7	8,3
Matemática	9	8,7	9,2
Física	8,4	8	9

Ao se retirar os significados das linhas e colunas, tem-se a matriz:

$$\begin{bmatrix} 7,5 & 7 & 8,3 \\ 9 & 8,7 & 9,2 \\ 8,4 & 8 & 9 \end{bmatrix}$$

Os valores dispostos são denominados *entradas* ou *elementos* de uma matriz. Esses elementos podem ser números (reais ou complexos), funções ou ainda outras matrizes. As *linhas* de uma matriz são as listas horizontais e as *colunas* são as listas verticais e determinam o tamanho da matriz, também conhecido como *ordem* da matriz.

Representa-se uma matriz A de m linhas e n colunas por:

$$A_{mxn} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix}$$

Onde no índice da cada um dos elementos estão sempre, respectivamente, o número da linha e o número da coluna, determinando, assim, a ordem da matriz. Alguns exemplos de matrizes:

$$\mathrm{A}_{3x2} = \begin{bmatrix} 1 & 4 \\ 5 & 3 \\ -2 & 6 \end{bmatrix} \qquad B_{2x3} = \begin{bmatrix} 9 & 1 & 0 \\ 7 & 2 & 5 \end{bmatrix} \qquad C_{1x3} = \begin{bmatrix} 2 & 8 & 0 \end{bmatrix}$$

$$D_{3x3} = \begin{bmatrix} \pi & -9 & \frac{1}{2} \\ 0 & 1,2 & 7 \\ 5 & 6 & 0 \end{bmatrix} \qquad E_{2x1} = \begin{bmatrix} 1 \\ 3 \end{bmatrix} \; F_{1x1} = \begin{bmatrix} 4 \end{bmatrix}$$

Duas matrizes A e B serão iguais somente se ambas forem de mesma ordem e se os seus elementos correspondentes forem iguais. Uma matriz de ordem nxn é dita **matriz quadrada de ordem n** e tem como **diagonal principal** os elementos

$$a_{11}, a_{22}, a_{33}, \cdots a_{nn}.$$

Uma matriz com apenas uma linha é denominada *matriz linha* e uma matriz com apenas uma coluna é denominada *matriz coluna*. Diz-se que uma matriz que tem todos seus elementos iguais a zero é uma *matriz nula* ou *matriz zero*. Se A for uma matriz de ordem $m \times n$ onde $n = m$, diz-se que A é uma *matriz quadrada* de ordem n. Se uma matriz quadrada tiver suas entradas da diagonal principal iguais a 1 e as demais entradas iguais 0, será denominada *matriz*

identidade. Alguns exemplos de matriz identidade:

$$\begin{bmatrix}1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}.$$

Denota-se uma matriz identidade de tamanho $n \times n$ por I_n. Na aritmética matricial uma matriz identidade exerce a função de "elemento neutro"na multiplicação de matrizes, ou seja, $I_nA = A = AI_n$.

Para uma matriz A qualquer de ordem $m \times n$ é possível determinar sua transposta, denotada por A^T, como sendo a matriz de ordem $n \times m$ que resulta da troca da posição das linhas e colunas de A. Por exemplo, considerando a matriz

$A = \begin{bmatrix}3 & 7 & 9\\ 1 & 4 & 8\end{bmatrix}$ tem-se que sua transposta é a matriz $A^T = \begin{bmatrix}3 & 1\\ 7 & 4\\ 9 & 8\end{bmatrix}$.

2.2.2 Operações com Matrizes

Uma vez que existem muitas aplicações para o conteúdo de matrizes, faz-se necessário existir "aritmética"envolvendo matrizes de forma que possam ser somadas, subraídas e multiplicadas de forma proveitosa. Nesta seção será desenvolvida tal aritmética.

2.2.2.1 Soma de Matrizes

Se A e B são matrizes de mesma ordem, diga-se mxn. A soma de A e B é a matriz denotada por $A + B$ cujos elementos são as somas dos elementos correspondentes de A e B. Por exemplo, considerando as matrizes

$$A = \begin{bmatrix}1 & 5 & 6\\ 0 & -2 & 8\\ 3 & 4 & 1\end{bmatrix} \text{ e } B = \begin{bmatrix}9 & 0 & 7\\ 6 & 8 & 1\\ 2 & 5 & 3\end{bmatrix},$$

tem-se que

$$A+B=\begin{bmatrix}1+9 & 5+0 & 6+7\\ 0+6 & -2+8 & 8+1\\ 3+2 & 4+5 & 1+3\end{bmatrix}=\begin{bmatrix}10 & 5 & 13\\ 6 & -6 & 9\\ 5 & 9 & 4\end{bmatrix}$$

e

$$A-B=\begin{bmatrix}1-9 & 5-0 & 6-7\\ 0-6 & -2-8 & 8-1\\ 3-2 & 4-5 & 1-3\end{bmatrix}=\begin{bmatrix}-8 & 5 & -1\\ -6 & -10 & 7\\ 1 & -1 & -2\end{bmatrix}$$

Observa-se que estas operações não estão definidas para matrizes de ordens diferentes pois os tamanhos não seriam compatíveis para efetuar estas operações. Portanto, a soma e subtração de matrizes está definida apenas para matrizes de mesma ordem.

2.2.2.2 Multiplicação de Matriz por um Escalar

Se A for uma matriz e k um escalar, a multiplicação da matriz A pelo escalar k, denotado por kA, é a matriz obtida ao se multiplicar cada entrada de A por k.

Por exemplo, considerando as matrizes

$$A=\begin{bmatrix}2 & 0 & 5\\ 7 & 3 & 1\end{bmatrix}, B=\begin{bmatrix}3 & 8\\ 4 & 6\end{bmatrix}$$

tem-se que

$$2A=\begin{bmatrix}2\times 4 & 2\times 0 & 2\times 5\\ 2\times 7 & 2\times 3 & 2\times 1\end{bmatrix}=\begin{bmatrix}8 & 0 & 10\\ 14 & 6 & 2\end{bmatrix}$$

e

$$3B=\begin{bmatrix}3\times 3 & 3\times 8\\ 3\times 4 & 3\times 6\end{bmatrix}=\begin{bmatrix}9 & 24\\ 12 & 12\end{bmatrix}$$

2.2.2.3 Multiplicação de Matrizes

Se A for uma matriz de ordem $m \times p$ e B for uma matriz de ordem $p \times n$, então o produto $A \times B$ é a matriz $m \times n$ cujas entradas são calculadas da seguinte forma: para obter a entrada da linha i e coluna j de $A \times B$ é preciso destacar a linha i de A e a coluna J de B, multiplicar as entradas correspondentes da linha e da coluna e, por último, somar os produtos resultantes. Por exemplo, considerando as matrizes

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \text{ e } B = \begin{bmatrix} 2 & 4 & 6 \\ 1 & 3 & 5 \end{bmatrix}$$

Tem-se que

$$A \times B = \begin{bmatrix} 1 \times 2 + 2 \times 1 & 1 \times 4 + 2 \times 3 & 1 \times 6 + 2 \times 5 \\ 3 \times 2 + 4 \times 1 & 3 \times 4 + 4 \times 3 & 3 \times 6 + 4 \times 5 \end{bmatrix} =$$

$$= \begin{bmatrix} 2+2 & 4+6 & 6+10 \\ 6+4 & 12+12 & 18+20 \end{bmatrix} = \begin{bmatrix} 4 & 10 & 16 \\ 10 & 24 & 38 \end{bmatrix}$$

Para que seja possível a multiplicação de duas matrizes é necessário que o número de linhas da primeira matriz seja igual ao número de colunas da segunda. Se esta condição não for satisfeita, o produto não estará definido.

2.2.2.4 Determinante de uma Matriz

O determinante de uma matriz $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ é obtido calculando $a_{11}a_{22} - a_{12}a_{21}$.

2.2.2.5 Matriz Inversa

Uma matriz B é inversa de uma matriz A se, quando multiplicada pela matriz A, resulta em uma matriz identidade, tal que $AB = BA = I$. Dessa forma, diz-se que A e B são inversas

uma da outra. Para uma matriz A ter uma matriz inversa, ela deve ser uma matriz quadrada e seu determinante ($det(A)$) não pode ser igual a zero e se B e C forem ambas matrizes inversas de A significa que $B = C$. A matriz B inversa de uma matriz A de ordem 2×2 é denotada por A^{-1} e é dada por

$$A^{-1} = \frac{1}{det(A)} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}.$$

2.2.3 Aritmética Modular

Aritmética modular é uma ferramenta importante em criptografia, pois permite a construção de algoritmos robustos e eficientes para proteger informações sensíveis. No método a ser utilizado nessa aplicação- a cifra de Hill- explorara-se bastante esse conhecimento. Como conceito, entende-se como um ramo da matemática que lida com operações em conjuntos finitos de números. Segundo (CARVALHO et al., 2015) em sua essência, trata-se de conceitos de divisibilidade e congruência em conjuntos de números inteiros. O foco está em calcular o resto da divisão de um número por outro e ao final, se determina a congruência entre dividendo e resto.

Neste contexto, se aprofundará essa definição apropriando-se do módulo 26 uma vez que, tem por objetivo converter as 26 letras do alfabeto em um conjunto de números inteiros e sucessivos dessa mesma quantidade de elementos. Após os cálculos matriciais, é bem comum que o resultado que deveria está dentro desse conjunto numérico, acabe sendo um elemento que não pertença ao conjunto anteriormente citado. No entanto, através dessa ferramenta matemática é possível encontrar o elemento correspondente ao valor encontrado mas que esteja dentro do conjunto objetivado.

Por exemplo, o número 27 é equivalente a 1 (27 mod 26 = 1) pois 27= 1.26 +1 (onde o resto da divisão é o valor correspondente). Já o número -1 é equivalente a 25 (-1 mod 26 = 25) uma vez que, -1= (-1).26 +25 resultando na afirmativa bicondicional que -1 é equivalente a 25.

2.3 Cifra de Hill

A cifra de Hill é um sistema de criptografia simétrica que utiliza matrizes para cifrar e decifrar mensagens. Foi inventada pelo matemático Lester S. Hill em 1929. A cifra de Hill é uma cifra poligráfica, ou seja, um conjunto de letras serão substituídas por um conjunto de números. Neste método cada letra do alfabeto é atribuída a um número.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Figura 7: Correspondência entre letras e números
Fonte: Os Autores (2023)

Após substituir cada letra da mensagem a ser cifrada por seu número correspondente, escolhe-se uma matriz quadrada de ordem n inversível para servir de chave. É necessário que a mensagem seja escrita em letras maiúsculas e que sejam ignorados acentos e possíveis espaços. Em seguida, agrupa-se os números em blocos de n letras que serão convertidos em matriz coluna. Multiplica-se a matriz chave por cada uma das matrizes coluna formadas a partir dos blocos de números gerando novas matrizes e aplica-se o *módulo n* cujos elementos formarão a mensagem cifrada. Por último, retornar os números para as letras correspondentes e assim obter a mensagem cifrada.

2.4 O uso de softwares educacionais no ensino da matemática

O mundo digital tem se tornado parte significativa do cotidiano de um grande número de pessoas, principalmente das gerações mais novas. Nesse contexto, é preciso encontrar formas de estender as vantagens tecnológicas, que facilitam e melhoram a vida das pessoas, ao campo da Educação Matemática. O uso de softwares no ensino da matemática pode ser muito vantajoso, possibilitando um processo ensino-aprendizagem mais dinâmico e interessante pois contribui para a visualização de conceitos abstratos, tornando-os mais concretos e compreensíveis para os alunos, segundo destaca Machado (2011). É importante ressaltar que, para que a utilização de softwares nas aulas de matemática seja plenamente proveitosa, é necessário que o software escolhido esteja alinhado com o conteúdo a ser ministrado e que seja adequado para suprimir as dificuldades identificadas pelo professor nos alunos, como evidencia Gomes

et al. (2002)

2.5 O uso de softwares computacionais no estudo de Criptografia

A utilização dos software computacionais têm um papel muito importante no estudo e na aplicação da criptografia. Uma vez que, esta é a ciência que está diretamente ligada ao intuito de proteger informações sensíveis por meio da transformação das mesmas para um formato ilegível, que só pode ser decifrado por pessoas autorizadas que possuem a chave de descriptografia apropriada. Esses utilitários são aplicados em vários viés tendo em vista que a criptografia se trata de uma área de conhecimento abrangente. O desenvolvimento de Algorítimos criptográficos, testes de segurança e gestão de chaves são alguns bons exemplos dessas aplicações.

Segundo destaca Cordeiro et al. (2011), com a grande aceitação da sociedade pelos modelos digitais de informação, a preocupação com a integridade do conteúdo em formato digital também deve ser considerável uma vez que, é extremamente vulnerável a intervenções não autorizadas (perda, adulteração e destruição). Diante disso, observa-se que a área de estudo que se aperfeiçoa na gestão de chaves criptográficas merece uma atenção especial pois deve gerar, armazenar e distribuir chaves criptográficas de maneira segura.

No desenvolvimento de Algoritmos Criptográficos, os matemáticos podem usar linguagens de programação como C++, Python ou MATLAB para criar protótipos e simulações. Quanto aos testes de segurança, são feitas avaliações de penetração e de segurança com o auxílio de software. São utilizadas também, ferramentas de varredura de vulnerabilidades e programas de quebra de criptografia.

2.6 Software Geogebra como ferramenta pedagógica

O Geogebra é um software educacional que reúne conceitos matemáticos de geometria, álgebra, estatística, cálculo diferencial e integral, entre outros conceitos. Foi desenvolvido com o objetivo de ser um facilitador no processo de ensino-aprendizagem de matemática e, é atualmente amplamente utilizado por professores com o objetivo de tornar as aulas mais dinâmicas e visuais, além de que também auxilia na preparação de materiais personalizados pelos

professores para suas aulas, como a construção de exercícios e tutoriais. Entre suas principais características estão: a integração Geometria e Álgebra que possibilita a combinação de expressões algébricas com objetos geométricos; o seu dinamismo que proporciona a experiência de aprendizado interativa; a criação de gráficos de funções matemáticas; dentre outras.

Além de possuir uma versão desktop e uma versão para dispositivos móveis, possui também uma plataforma online, que apesar de oferecer menos funções ainda é bastante abrangente em ferramentas matemáticas. Sua versão online permite aos usuários criar projetos matemáticos e compartilhá-los, além de poder colaborar em outros projetos. Um dos principais motivos de essa ferramenta ser bastante escolhida como um facilitador didático está na sua acessibilidade - é um software bem completo, com interface intuitiva e dinâmica, de código aberto e disponível gratuitamente sendo assim, acessível para diversos públicos.

Tendo em consideração que este trabalho propõe a Cifra de Hill (um algoritmo criptográfico que envolve a transformação de blocos de texto em cifras usando matrizes) como abordagem pedagógica para o ensino de matrizes, o software Geogebra apresenta-se como uma excelente ferramenta para utilização durante as aulas deste conteúdo, uma vez que possui entre suas ferramentas a multiplicação de matrizes que é a base para a cifragem de mensagens utilizando este método criptográfico.

Para os cálculos matriciais no Software, o aprendiz precisa inserir esse ente matemático na plataforma. Vale ainda ressaltar que, é importante nomear algebricamente cada entrada como por exemplo a "matriz chave"uma vez que, será massivamente repetida durante os cálculos. Para nomear qualquer entrada, basta escolher uma letra que deverá vir seguida do sinal de igualdade. No caso das matrizes, já estando nomeada e com o sinal a espera dos valores, dá-se entrada sempre entre o sinal de chaves. Para inserir as linhas da organização tabular, deve-se abrir mais um conjunto de chaves pra cada nova linha estando essas separadas por virgulas. As colunas por sua vez, se dão através de virgulas que separaram dos valores da linha anteriormente inserida.

Para exemplo prático, será tomada por exemplo a matriz A = $\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$ que deverá ser inserida como mostra a imagem a seguir:

Para a continuidade do calculo, é necessário inserir o comando de determinante de matrizes para saber se a matriz chave inserida possui determinante diferente de zero uma vez que, essa é a condição para que a matriz chave possua a inversa permitindo assim, descriptografar a

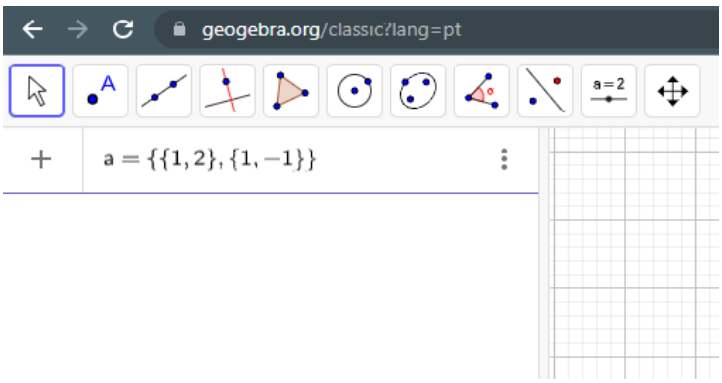

Figura 8: Inserindo matriz no Geogebra
Fonte: Os Autores (2024)

mensagem cifrada. A forma mais simples de dar essa entrada é digitando "determinante(nome da matriz)". No contexto presente, para calcular o determinante da matriz A, basta digitar determinante (a). A multiplicação de matrizes é o ponto fundamental para que esse método seja desenvolvido e esta operação no Geogebra se dá nos seguintes passos: primeiramente, deve-se observar se ambas as matrizes estão devidamente inseridas. Em segundo lugar, escolher uma letra para nomear o resultado da operação. Ao final, cabe somente a expressão algébrica coerente. Por exemplo: ao multiplicar a matriz chave A por uma matriz coluna C = $\begin{pmatrix} 3 \\ 7 \end{pmatrix}$ se obterá uma matriz resultante que será chamada de D. Para que isso ocorra na devida forma, cabe inserir a expressão como mostra a imagem 9.

Para que a mensagem cifrada seja passível de decifração no método de Hill, se utilizará a inversa da matriz chave. Como já foi referido, para que uma matriz qualquer possua inversa, é condição necessária que o determinante dessa seja diferente de zero. Dando prosseguimento ao exemplo discorrido, tem-se que o determinante de a é igual a -3 que por sua vez, significa que a referida chave possui matriz inversa. Para calcular a inversa de A, basta inserir o comando "invert(nome da matriz)". Com o objetivo organizacional, a nova matriz será nomeada com a letra e. O comando inserido corretamente pode ser conferido na figura de número 10.

Mediante o contexto apresentado, cabe considerar que o software Geogebra é uma ferramenta extremamente versátil e útil para ser usado como plataforma facilitadora no ensino matemático de modo geral uma vez que, apresenta uma gama bem diversificada de possibilidades nas mais variadas especialidades de cálculos. Quanto a presente abordagem pedagógica, pode-se considerar a hipótese que o Geogebra satisfaz as condições e possibilidades para ser a ferramenta simplificadora para o desenvolvimento da criptografia que visa auxiliar no ensino

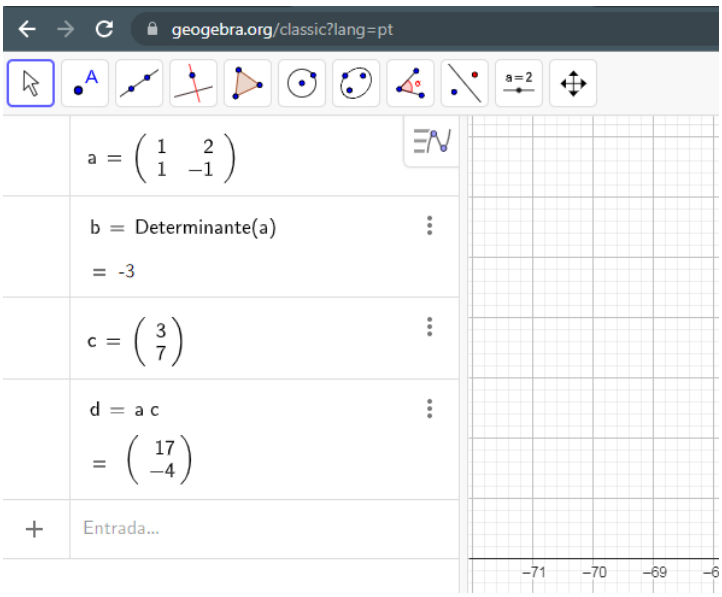

Figura 9: Multiplicação de matrizes no Geogebra
Fonte: Os Autores (2024)

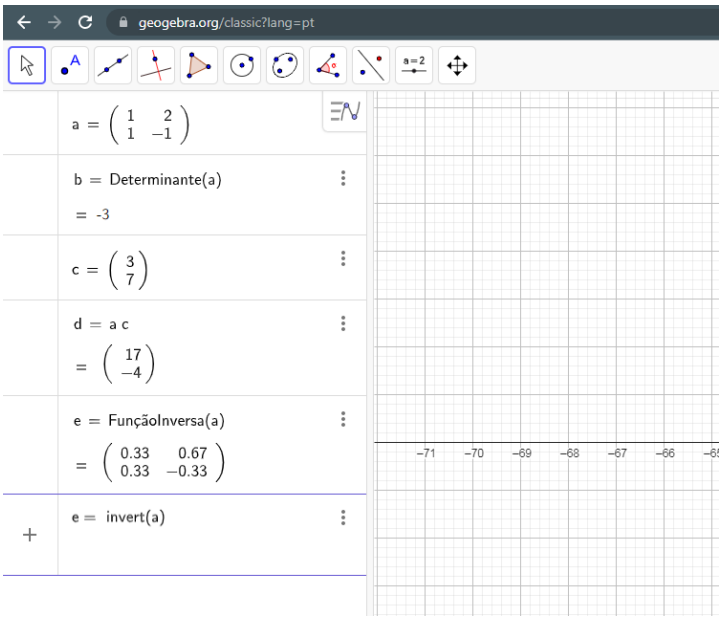

Figura 10: Inversa da matriz no Geogebra
Fonte: Os Autores (2024)

das matrizes. Não obstante, ainda traz um contexto motivacional uma vez que, o conteúdo que normalmente é explicado através do método tradicional, passa a ser tecnológico e atraente. Quanto a possibilidade de evolução dessa mesma abordagem com o auxílio de outra interface, é consideravelmente possível desde que essa outra, também carregue as possibilidades

matemáticas citadas anteriormente.

3 PROCEDIMENTOS METODOLÓGICOS

3.1 Classificação da pesquisa

O presente trabalho baseia-se em uma pesquisa aplicada, pois tem seu interesse posto em realizar um diagnóstico de uma determinada situação, mediante isto, identificar um problema específico e buscar promover conhecimento que possibilite a apresentação de uma proposta de solução para o problema, através de uma aplicação prática (NASCIMENTO; SOUSA, 2016). Possui uma abordagem metodológica quali-quantitativa, com objetivo exploratório, que tem se mostrado o método de pesquisa mais utilizado por pesquisadores da área da educação, uma vez que possibilita o envolvimento do pesquisador no contexto da investigação, aproximando-o do seu objeto de estudo - o que acredita-se ser indispensável para uma melhor construção de conhecimento do fato estudado. Além disso, esse método atende ao fato de que no processo de ensino-aprendizagem as coisas acontecem de forma dinâmica, no sentido de que são muitas as particularidades compreendidas neste contexto e que , portanto, as variáveis envolvidas não devem ser estudadas de forma isolada, atribuindo-se a elas somente uma dimensão quantificável. (ANA; LEMOS, 2018)

3.2 Método de Trabalho

3.2.1 Conscientização do problema

De acordo com a Lei de Diretrizes e Bases da Educação Nacional (Lei nº 9.394/96) (FEDERAL, 2005), o Ensino Médio tem entre suas principais finalidades o aprofundamento dos conhecimentos obtidos no Ensino Fundamental, a preparação do estudante para o trabalho e para o exercício da cidadania, sua formação ética e a compreensão dos processos produtivos, relacionando a teoria com a prática no ensino de cada disciplina e, em uma de suas diretrizes determina que as metodologias de ensino e de avaliação adotadas para o Ensino Médio deverão estimular a iniciativa dos estudantes. Diante disso, percebe-se que, atualmente, o ensino puramente disciplinar pode não ser o mais adequado para atender à essas diretrizes e os métodos tradicionais (quadro, caderno, aula expositiva), quando realizados sem propostas de aplicações práticas na realidade dos estudantes podem dificultar a aprendizagem, uma vez que

não contribuem para o desenvolvimento de competências e habilidades de forma interdisciplinar e não possibilitam o constante uso de tecnologias no processo ensino-aprendizagem, o que tem se tornado indispensável, dado que o uso dela está intrínseco a realidade dos alunos deste tempo presente.(LAUDARES; LACHINI, 2000)

Momentos de diversão que outrora eram feitos de forma presencial e motora, hoje já se dão de forma tecnológica e online. Tendo em vista a constante evolução das pessoas em situações simples como o momento de lazer, se faz necessário que a metodologia usada no processo de ensino- aprendizagem também evolua para que possibilite a motivação do aluno e com isso viabilize a aprendizagem.

A carência de contextualização dos conteúdos de Matemática ensinados no Ensino Médio tem causado um constante questionamento por parte dos estudantes: onde irei aplicar esse conhecimento na vida prática? Se não há aplicação, por que devo aprender Matemática? Entretanto, segundo Moreira (1996) destacam os PCNEM's (Parâmetros Curriculares Nacionais do Ensino Médio), o conhecimento desta disciplina pode contribuir de várias formas para a vida do indivíduo, pois o pleno conhecimento de sua sistematização torna o indivíduo mais crítico e perspicaz diante de situações de problemas da vida real visto que, dentre outras contribuições, o aprofundamento do conhecimento em Matemática, ou seja, a continuidade do estudo da disciplina, só se dá mediante a compreensão do conteúdo anterior pois se desenvolve de forma sucessiva e organizada, o que pode contribuir para o desenvolvimento de habilidades e competências essenciais que possibilitem os alunos estabelecerem relações que os auxiliarão a resolver problemas cotidianos.

No entanto, atualmente, a maneira de ensinar Matemática não tem levado o aluno a uma aprendizagem efetiva pois, em muitos casos os conteúdos sofrem com a indiferença dos alunos por conta da visão tradicionalista do ensino da matemática, tendo em vista a dissonância dos exemplos utilizados com relação a realidade dos alunos considerando que estão inseridos em um mundo em constante processo de inovação (PONTES, 2013). Para a conscientização deste problema, tornou-se necessário uma apresentação de uma proposta pedagógica de intervenção que, por sua vez, despertou os alunos a perceberem que podem ter aulas dos mesmos conteúdos já estudados, no entanto, de forma mais dinâmica e contextualizada, visando as situações de vida prática para que possam ser correlacionadas com a teoria exposta em sala de aula. Com essa finalidade, foi realizada uma palestra com alunos da 2ª série do Ensino Médio do Colégio Militar Tiradentes II com o intuito de promover essa conscientização a respeito do ensino da matemática e como ele pode ser interessante. Foi apresentado o conteúdo de

Criptografia e sua fundamentação matemática como sugestão de aplicação para o conteúdo de Matrizes.

3.2.2 Sugestão

Inicialmente, foi de considerável importância ressaltar a problemática sobre a qual este trabalho se desenvolve, afinal sob esta ótica foi difundida a conscientização sobre os problemas enfrentados por discentes e docentes no decurso da troca de conhecimento em relação ao tema matemático das matrizes. Dentre diversos contextos, Pontes (2013) destaca que este assunto, normalmente é difundido sem promover a perspicácia do aluno, uma vez que enfatiza somente a memorização de fórmulas, conceitos e resolução de exercícios isolados fazendo, assim, com que o aluno não consiga progredir intelectualmente pois ele não será capaz de aplicar esse conhecimento em situações práticas que vão além daquilo que foi exercitado de forma mecânica e com pouca ênfase na compreensão plena do conteúdo. Em consideração a isso, verificou-se que o conteúdo de Matrizes, ministrado no Ensino Médio, pode se mostrar aplicável em diversos contextos de forma que possibilite maior compreensão por parte dos estudantes e, desta forma optou-se por discorrer este trabalho científico neste viés: amadurecer o conteúdo de Matrizes através de uma proposta de atividade que mostre uma possibilidade de aplicação prática deste conteúdo.

Para realizar a conscientização do problema que envolve o ensino de matrizes, foi promovida uma palestra em uma escola para educadores e estudantes do Ensino Médio destacando a importância da contextualização e como isso pode melhorar a compreensão e aplicação desse conteúdo além de objetivar a proposta do estudo da criptografia como uma possível abordagem para a aplicação deste conceito, salientando sua íntima relação com o tema. Ressaltando ainda, as dificuldades que o docente está sujeito quando ele mesmo se propõe a transcender as formas de ensino mais tradicionais, tendo em vista a pouca oferta de estrutura e recursos adequados nas instituições de ensino para que possibilitem essa sugerida contextualização do conteúdo anteriormente mencionado, pois essa forma de abordagem está normalmente mais correlacionada ao cenário da tecnologia.

Tendo em vista a extensão do conteúdo de matrizes e buscando objetivar e o tornar eficaz, foi feito um crivo de quais entes deste conteúdo estão intrínsecos ao estudo da codificação e decodificação de mensagens. Procedendo assim, efetuou-se uma revisão desses conceitos matriciais básicos em sala de aula através de uma aula expositiva e demonstrou-se

como podem ser usados na criptografia, visando a apresentação de exemplos e analogias simples para a compreensão da matéria e como esses conceitos podem ser aprendidos de forma interessante.

3.2.3 Desenvolvimento

O presente tópico tem o intuito de definir e detalhar os objetivos específicos deste trabalho que tem como objetivo geral **propor uma abordagem pedagógica para o estudo de Matrizes no Ensino Médio que envolva a criptografia**.

Visando alcançar o objetivo central desta pesquisa, definiu-se os seguintes objetivos específicos:

1. **Realizar um levantamento bibliográfico sobre a história da criptografia, sua importância para a segurança da informação e sua estreita relação com a Matemática;**

   Esta é uma etapa crucial na pesquisa acadêmica, pois tem o objetivo de revisar a literatura existente a respeito do tema de interesse. Antes de tudo foi importante que houvesse a definição da pergunta de pesquisa para que fosse possível a realização do levantamento bibliográfico e que esse fosse feito de forma eficaz possibilitando a definição do tema do trabalho. Em consideração a isso, decidiu-se por a pergunta de pesquisa: "qual a eficácia de uma abordagem pedagógica no ensino de matrizes para estudantes do Ensino Médio, considerando a compreensão conceitual, a aplicação prática e o engajamento dos alunos?". Assim sendo, logo após realizar buscas sobre a pergunta de pesquisa, foram encontrados títulos que ligavam a criptografia ao conteúdo de matrizes. Logo, definiu-se o tema: Criptografia: uma abordagem pedagógica para o estudo de Matrizes no Ensino Médio. Visando o recolhimento do material bibliográfico e utilizando-se de palavras - chave como criptografia, matrizes, Ensino Médio, abordagens pedagógicas e afins, foram selecionados títulos que serviram de base teórica para a construção do trabalho e para enriquecê-lo mais ainda, utilizou-se uma técnica amplamente conhecida e difundida: técnica snowball. Também conhecida como "bola de neve"em português, esta é dita por Silva et al. (2019) como sendo extremamente utilizada em pesquisas bibliográficas pois identifica referências adicionais e relevantes. Essa técnica é especialmente útil para encontrar trabalhos menos conhecidos ou que não estão facilmente disponíveis em bases de dados tradicionais.

Como principal base de dados a ser consultada estabeleceu-se o Google Scholar, primeiramente, por se tratar de uma fonte de informação com bastante credibilidade e que visa facilitar o referencial teórico para diversas linguagens de escrita acadêmicas. Além disso, destaca-se por sua ampla gama de trabalhos científicos em sua base de dados.

2. **Revisar conceitos básicos e essenciais de Matrizes ligando-os a sua aplicação na criptografia;**

   Ligar os conceitos básicos de matrizes à aplicação na criptografia envolve entender como as operações matriciais são utilizadas no processo de cifragem e decifração de mensagens. Para isso, tornou-se necessário realizar uma revisão dos conceitos básicos e essenciais de matrizes para alicerçar a proposta deste trabalho. Para alcançar tal objetivo, foi importante primeiro compreender o que são matrizes e para esse propósito, foram realizadas aulas expositivas para uma turma do segundo ano do Ensino Médio sobre conceitos básicos de Matrizes partindo da definição, elementos, ordem de uma matriz, matriz inversa, trabalhando também com as operações básicas matriciais, como soma, multiplicação por um escalar e multiplicação de matrizes.

   Como forma de fixação dos conceitos ministrados, foram realizados exercícios propostos envolvendo as operações matriciais com o uso do quadro, papel e lápis com o intuito de garantir um bom alicerce para o aluno e que o proporcionasse compreender plenamente os processos criptográficos que requerem tais conceitos. Além disso, ainda durante as aulas expositivas, após as conceituações, foi introduzido um processo de cifragem e decifração de uma mensagem aleatória com a ajuda dos estudantes.

3. **Apresentar os dados levantados em uma palestra para docentes e discentes do Ensino Médio;**

   Sabe-se que as palestras são ferramentas poderosas e eficazes quando se tem por objetivo a conscientização de problemas a respeito de um determinado tema. Por esse motivo, foi realizada uma palestra a respeito da origem e o desenvolvimento da criptografia, citando cifras famosas, fatos históricos importantes que envolveram a criptografia, como seu estudo foi fundamental para o avanço significativo da tecnologia nos últimos anos, sua importância para a segurança da informação destacando seu uso imensurável no dia a dia da humanidade e evidenciando ferramentas presentes na vida dos estudantes, como por exemplo *Whatsapp, Instagram, Facebook* para os confrontar sobre o conhecimento prévio a respeito do que seria a criptografia utilizada nessas ferramentas.

   Além de focalizar todo o contexto da criptografia, foi oportunizada a reflexão a respeito

dos métodos pedagógicos utilizados para a difusão do conhecimento nos dias atuais, sobretudo acerca da Matemática, tendo em vista que sua maioria se dá apenas na forma de conceitos decorados, reproduzidos e descontextualizados, visando a conscientização do problema de pesquisa deste trabalho. E, ao final, expôs-se a proposta de abordagem de criptografia para o ensino de matrizes.

4. **Promover uma proposta de atividade envolvendo o conteúdo de Matrizes aplicado em criptografia com o auxílio do Software GeoGebra;**

   Na tentativa de tornar o aprendizado mais envolvente para os alunos, foi promovida uma atividade envolvendo o conteúdo de Matrizes aplicado em criptografia com o auxílio do Software GeoGebra visando ser uma abordagem eficaz de tornar o aprendizado mais dinâmico e prático para os discentes. Os materiais necessários para a realização dessa atividade foram computadores com acesso à internet que garantissem o acesso ao software GeoGebra, um datashow, quadro branco e pincéis.

   Em um primeiro momento foi apresentado aos alunos o Software GeoGebra, destacando suas funções no que se refere às matrizes, estimulando-os a criarem matrizes simples e realizar operações básicas. Em seguida, mostrou-se um exemplo simples de como transformar uma mensagem em matriz e multiplicá-la por outra matriz para criptografar e, posteriormente, realizar o processo inverso.

   Na sequência, pretendendo finalizar a atividade da forma mais satisfatória possível, proporcionou-se a oportunidade para os alunos compartilharem suas experiências com o GeoGebra e explanarem como isso facilitou o entendimento dos conceitos além de conduzi-los a uma discussão a respeito do que acharam da proposta de abordagem para o ensino de matrizes.

5. **Avaliar a aplicação do trabalho por meio de questionários;**

   A avaliação da aplicação do trabalho por meio de questionários é uma prática comum em diversos contextos: empresas, organizações, instituições de ensino e pesquisas acadêmicas. Essa abordagem oferece uma maneira sistemática de coletar *feedback* e obter *insights* sobre a eficácia de um trabalho ou projeto.

   Visando descobrir qual a avaliação dos alunos em relação a abordagem proposta por esta pesquisa para o ensino de matrizes, foram elaborados questionários, que foram respondidos pelos discentes, com perguntas bem direcionadas quanto ao desempenho da proposta tendo como foco a clareza das explicações durante as aulas, o envolvimento dos alunos e a utilidade prática da criptografia. Vale ressaltar ainda, que houve um

espaço destinado a sugestões de melhoria permitindo que os alunos expressem suas opiniões sobre como a abordagem pedagógica poderia ser aprimorada.

6. **Apresentar os resultados por meio de relatos e gráficos estatísticos;**

   Para a apresentação dos resultados, utilizou-se do gráfico de palavras por se tratar de uma ferramenta versátil que pode ser personalizada de acordo com o contexto e o objetivo da análise. Além do mais, ajuda a destacar visualmente as palavras mais relevantes, facilitando a comunicação de informações importantes de forma concisa e atraente.

Para viabilizar a execução desta proposta como um todo, foi necessário destacar que o processo foi feito de forma sequenciada e organizada. Para isso, a aplicação no Colégio Militar Tiradentes II onde foi feita a abordagem piloto na forma de palestra, com objetivo de captar apoiadores dessa iniciativa tanto da parte dos discentes quanto da parte docente e administrativa da escola. Os discentes, por sua vez, se mobilizaram em participar do projeto na forma de ouvintes e contribuintes diretos, ou seja, foram a parte entrevistada e experimentada e por sua vez, contribuíram com "feedbacks"diretos e indiretos para o recolhimento de dados que serviram como avaliativos a esta abordagem.

Em retorno a todo esse esforço, os alunos foram a parte beneficiada de modo mais significativo. Já o corpo docente e administrativo da escola, se mobilizou de tal forma que viabilizou o projeto, na forma de concessões: permissões; espaço físico; tempo; estrutura e afins. Aqueles que se propõem em desenvolver este projeto, tanto orientandos quanto orientador, se mobilizaram em preparar ferramentas e possibilidades para que este projeto se desenvolvesse da melhor forma possível que vão desde arcabouço teórico, organização, preparação de slides para apresentações, materiais lúdicos ou tecnológicos, preparação de aulas, questionários e afins. vale ainda ressaltar que toda e estrutura que não foram concedida pelas partes beneficiadas, foram viabilizadas por este ultimo grupo mencionado.

3.2.4 Avaliação

A avaliação de uma abordagem pedagógica que utiliza criptografia para o ensino de matrizes no Ensino Médio deve ter foco em medir a compreensão dos discentes a respeito dos conteúdos criptografia e matrizes além da capacidade de relacionar os dois conteúdos. Dentre outras formas de avaliar essa abordagem, destaca-se os seguintes critérios:

- **Avaliação sobre a compreensão dos alunos sobre o papel da criptografia;**

  Foi realizada através de discussões em sala de aula e análise das respostas dos estudantes aos questionários.

- **A capacidade desenvolvida dos alunos para resolver desafios práticos que exijam que os mesmos usem operações de matrizes para encriptar e decriptar mensagens;**

  Foi realizada através de exercícios propostos em sala de aula mediante observação.

- **Avaliação de Compreensão do Contexto Histórico da Criptografia;**

  Foi realizada através de discussões em sala de aula.

- **Avaliação da colaboração dos alunos em projetos de equipe;**

  Foi realizada através da observação da interação dos alunos entre si durante o momento de aplicação da abordagem de criptografia.

- **Avaliar se os alunos compreenderam os conceitos fundamentais de criptografia e matrizes;**

  Foi realizado mediante a observação do desempenho dos alunos durante a execução das atividades.

- **Avaliar se os materiais didáticos utilizados são eficazes em transmitir os conceitos de criptografia e matrizes;**

  Foi realizado através da observação de como os recursos didáticos foram eficazes durante a aplicação da abordagem.

- **Avaliação da abordagem pedagógica pelo ponto de vista dos estudantes.**

  Foi realizado através do *feedback* dos alunos, permitindo que expressem suas opiniões e sugestões em relação ao método de ensino.

3.2.5 Apresentação dos resultados

Após realizar todos os procedimentos de avaliação deste trabalho, coletar e analisar os resultados obtidos, tais resultados foram tabulados e apresentados em gráficos e tabelas de forma visualmente atraentes destacando os principais resultados como: a compreensão dos conceitos de matrizes, proporcionando uma ideia da quantidade de alunos que tiveram uma

boa compreensão do conteúdo; a aplicação na criptografia mostrando a ideia da quantidade de alunos que realizaram uma aplicação bem-sucedida; um gráfico que mostre o engajamento dos alunos antes e depois da implementação da abordagem pedagógica; a avaliação dos alunos sobre a abordagem com a ideia da proporção de *feedback* positivo.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Neste capítulo será apresentado como se deu a aplicação da proposta pedagógica deste trabalho e discutidos os seus resultados.

4.1 Uma sequência didática para o processo de ensino-aprendizagem de Matrizes

O ensino de matrizes no Ensino Médio geralmente se concentra em compreender os conceitos básicos e realizar operações dando ênfase aos cálculos e à memorização de regras (SIQUEIRA et al., 2020). Os tópicos mais comumente abordados são definição e notação, operações básicas como adição e subtração de matrizes, multiplicação de matriz por um escalar, matriz identidade e matriz inversa, entre outros. Esses tópicos são fundamentais não somente na área da álgebra linear, mas também em várias disciplinas como física, estatística, ciência da computação e engenharia. De fato, este é um conteúdo rico em aplicações práticas em diversas áreas do conhecimento, especialmente no universo digital que é tão presente na vida cotidiana dos estudantes do século XXI. No entanto, a sua desvinculação de aplicações práticas pode levar os alunos a questionarem a relevância e utilidade desses conceitos, pois muitas vezes os estudantes apresentam dificuldades para relacionar conceitos abstratos ao mundo real, daí a necessidade de evidenciar no ensino de matrizes suas aplicações em situações reais. Realizar a conexão deste conteúdo com aplicações do mundo real pode ajudar os alunos a verem a utilidade desses conceitos matriciais além da sala de aula e além disso, o uso da tecnologia pode facilitar a resolução de problemas envolvendo matrizes (SIQUEIRA et al., 2020). Portanto, melhorar o ensino de matrizes no Ensino Médio envolve adotar abordagens pedagógicas que enfatizem a contextualização e a sua aplicação prática.

Durante a fase de levantamento bibliográfico, percebeu-se que a criptografia tem, desde as suas primeiras aparições, um estreito relacionamento com a matemática e que atualmente utiliza-se de conceitos matemáticos para garantir a segurança da informação e entre as maneiras pelas quais a matemática é aplicada na criptografia está a Álgebra Linear. A partir disso, decidiu-se aprofundar os estudos na área de criptografia envolvendo álgebra linear e percebeu-se que para um bom aproveitamento deste trabalho, o tópico de matrizes e criptografia era o que mais satisfazia o objetivo da pesquisa, uma vez que é plenamente adaptável para os conteúdos ministrados no Ensino Médio, podendo contribuir para o aprendizado dos alunos e, assim, tornar o processo de ensino-aprendizagem mais interessante. Ainda durante o processo

de levantamento bibliográfico, ao estudar sobre a história da criptografia, tem-se o primeiro contato com a Cifra de Hill que é muito conhecida devido a sua utilização em um período em que os processos criptográficos baseavam-se em cálculos matemáticos não muito complexos mas que eram eficazes para a época e que por isso são de fácil compreensão. Dessa forma, a Cifra de Hill, cujo algoritmo se baseia em operações matriciais foi escolhida como a aplicação do conteúdo de matrizes a ser desenvolvida neste trabalho.

Além disso, era necessário lembrar aos alunos e aos professores a importância da Matemática no dia a dia da sociedade e, que devido a tamanha importância o estudo dessa disciplina torna-se indispensável e portanto, as metodologias de ensino de Matemática precisam estar alinhadas a essa realidade. Diante disso, decidiu-se que para introduzir aos alunos estes assuntos, seria necessário a realização de uma palestra com o tema: Criptografia e Matemática Protegendo Informações com Matrizes, que visava apresentar aos alunos a definição de criptografia, seu surgimento, um pouco de sua história, sua importância na atualidade, a sua relação com a matemática, definir e apresentar a Cifra de Hill como uma aplicação do conteúdo de matrizes, além de promover a reflexão a respeito da relevância da matemática no mundo atual e a necessidade de tornar o estudo desta disciplina tão importante mais prático e atrativo.

Para desenvolver a proposta deste trabalho, buscou-se uma instituição de Educação Básica do município de Imperatriz-Ma, que estivesse interessada no projeto e que possuísse em sua estrutura um laboratório de informática funcional, com computadores suficientes para atender a uma turma com uma média de 30 alunos. Em um primeiro momento, contactou-se a direção pedagógica do Colégio Militar Tiradentes II e, apesar da instituição mostrar-se muito interessada no projeto, era inviável a realização do trabalho nesta escola por conta da falta de um laboratório de informática que fosse útil para a realização do projeto.

Depois de visitar outras instituições e encontrar sempre a mesma situação, teve-se a ideia de utilizar o laboratório de informática da UEMASUL, campus Imperatriz e, após confirmar a disponibilidade do laboratório, decidiu-se propor ao Colégio Militar Tiradentes II que os seus alunos se deslocassem até à UEMASUL para participarem da aula, uma vez que as duas instituições encontram-se próximas fisicamente, o que facilitaria o deslocamento dos alunos até a Universidade.

A escola prontamente atendeu ao pedido e concordou com o deslocamento dos alunos. Ficou acordado que a palestra seria realizada na escola num período de duas horas-aula, dedicadas a disciplina de Aprofundamento em Matemática e suas tecnologias ministrada pela professora Gardenia, que concordou em ceder seus horários. A turma escolhida foi uma turma

de exatas do segundo ano do Ensino Médio devido ao fato de que o conteúdo de matrizes foi ministrado a essa turma no início do ano letivo. Ficou decidido ainda que, na semana seguinte, os alunos se deslocariam até a Uemasul para a aula no laboratório de informática durante os mesmos horários disponibilizados pela professora Gardenia, com acréscimo de um horário, cedido pelo professor Celso que ministra a disciplina de Matemática para essa turma, totalizando três horas-aula.

Após a confirmação da participação da escola no projeto, iniciou-se a prática do mesmo. Na mesma semana os autores deste trabalho estiveram no Colégio Militar Tiradentes II para ministrar a palestra. O evento contou com a participação de grande parte da turma e da professora Gardenia. Os recursos utilizados foram uma apresentação em PowerPoint produzida pelos palestrantes, o datashow disponível na sala de aula, um pendrive com o arquivo PowerPoint, um computador e os questionários impressos em folha A4.

Figura 11: Slide 1. Tema da palestra
Fonte: Os Autores (2023)

A palestra foi iniciada com a apresentação dos palestrantes, do professor orientador deste projeto e feitos os agradecimentos aos alunos pela participação e à professora pela disponibilização dos horários. Em seguida, já introduzindo os principais assuntos que envolvem o tema deste trabalho, foi apresentado o primeiro tópico intitulado "A Tecnologia no Mundo Atual", onde foi abordado um pouco sobre o papel fundamental que a tecnologia desempenha no dia a dia da sociedade em geral e como a tem moldado profundamente, como também a economia e a forma como acontecem as interações sociais.

Foram citadas e brevemente comentadas algumas áreas em que a tecnologia tem papel significativo, como na área da saúde com tecnologias médicas avançadas que produzem

ótimos equipamentos, proporcionam diagnósticos mais precisos e melhoram os tratamentos, na área da educação transformando a forma como as pessoas aprendem e têm acesso ao conhecimento, proporcionando diferentes experiências de aprendizado, na área da comunicação com as redes sociais, que facilitam o compartilhamento de informações, conectam pessoas no mundo inteiro e estão profundamente presentes no cotidiano dos estudantes através dos aplicativos de mensagens que tornam a comunicação instantânea possível a qualquer momento e em qualquer lugar; na área dos negócios e na economia com comércio eletrônico que facilita a compra e venda de produtos, eliminando as barreiras geográficas, na área de mídia e entretenimento com jogos eletrônicos e realidade virtual, entre muitas outras áreas que poderiam ser destacadas.

Para concluir este tópico, foi apresentado que os avanços tecnológicos são muito importantes para a área de segurança da informação, pois é uma área que precisa avançar de acordo com o desenvolvimento da tecnologia para garantir a proteção de dados e informações confidenciais. Justificou-se, então, o fato de que a tecnologia tem trazido muitos benefícios e que a sua existência é importante nos dias atuais e, portanto, o mundo digital continuará avançando.

Figura 12: Slide 2. Informações sobre os palestrantes
Fonte: Os Autores (2023)

Dando continuidade a palestra, com o objetivo de relacionar os avanços tecnológicos com a Matemática, o próximo tópico apresentado foi "A Importância da Matemática no Mundo Atual", onde foi destacado a relevância que esta ciência tem em diversas áreas e principalmente, como ela contribui para o desenvolvimento tecnológico pois permeia muitos aspectos do mundo moderno. Destacou-se que sua importância vai além das salas de aula e que não é, como alguns alunos costumam acreditar, uma disciplina que está no currículo

Figura 13: Slide do tópico: A Tecnologia No Mundo Atual
Fonte: Os Autores (2023)

do Ensino Médio somente para dificultar o desempenho dos estudantes, mas que os conceitos matemáticos apresentados em sala de aula têm, sim, suas utilidades no dia a dia das pessoas e influenciam diretamente o progresso de muitas áreas da vida como na pesquisa científica para formulação de teorias, modelagem de fenômenos, análise de dados experimentais. Comentou-se, também, como essa disciplina é profundamente utilizada na economia para tomadas de decisões a respeito de investimentos, como por exemplo, analisar mercados e calcular riscos e como ela é crucial para o desenvolvimento cognitivo e a resolução de problemas, uma vez que habilidades matemáticas são valorizadas em diversas profissões; além de suas diversas aplicações na medicina e saúde, auxiliando na pesquisa médica, modelagem de epidemias, análises estatísticas, entre outros.

Falou-se também sobre sua importância para a tecnologia moderna e como a Ciência da Computação está amplamente baseada em princípios matemáticos, citando exemplos como a programação e a segurança da informação, e que por isso essa disciplina é essencial para o mundo digital atual pois fornece as ferramentas e os conceitos necessários para promover o avanço contínuo na área da tecnologia da informação.

Diante da demonstração de sua importância, levantou-se uma reflexão sobre como acontece o ensino da Matemática nas escolas (PONTES, 2018). Uma vez que tal disciplina exerce relevância na atualidade, seu processo de ensino-aprendizagem precisa ser eficaz de forma que promova uma compreensão profunda dos seus conceitos e inspire nos estudantes um interesse duradouro pela matéria a fim de que possam desfrutar de todos os benefícios que o estudo da Matemática pode proporcionar a uma pessoa em sua vida na sociedade. Para isso, o próximo

Figura 14: Slide do tópico: A Importância Da Matemática No Mundo Atual
Fonte: Os Autores (2023)

tópico da palestra foi "A importância da contextualização no Ensino da Matemática", onde foi explicado como a aplicação prática dos conteúdos matemáticos estudados em sala de aula é fundamental no processo de ensino-aprendizagem tornando a disciplina mais envolvente, relevante e acessível para os alunos. Ao conectar a Matemática ao mundo real, os educadores podem inspirar uma apreciação mais profunda da disciplina e preparar os alunos para aplicar seus conhecimentos em diversas situações ao longo de sua vida equipando-os com habilidades essenciais para enfrentar os desafios do mundo real.

Algumas razões foram listadas com a intenção de mostrar como a aplicação prática pode ajudar no ensino da Matemática: ajuda os alunos a perceberem que a matemática está integrada em situações do mundo real e que ao estudá-la estarão se preparando para os desafios reais; contribui para a interdisciplinaridade, uma vez que envolve a integração de conceitos matemáticos com outras disciplinas; colabora com a motivação dos alunos em aprender e com o engajamento durante as aulas; proporciona uma compreensão mais profunda e plena do conteúdo; incentiva a colaboração entre os alunos ao promover o trabalho em equipe na resolução de problemas; entre outras razões.

Após comentar sobre a importância da contextualização no ensino da Matemática, foi exposto o tópico "Criptografia como exemplo", para mostrar uma aplicação prática de conteúdos matemáticos. Durante a explicação deste tópico, foi relatado que a criptografia é uma interessante aplicação prática de conteúdos matemáticos, pois os algorítimos criptográficos, que garantem a segurança da informação, têm raízes em conceitos matemáticos de Álgebra Linear e Teoria dos Números. Com esse tópico da palestra, foi mostrado que a aplicabilidade

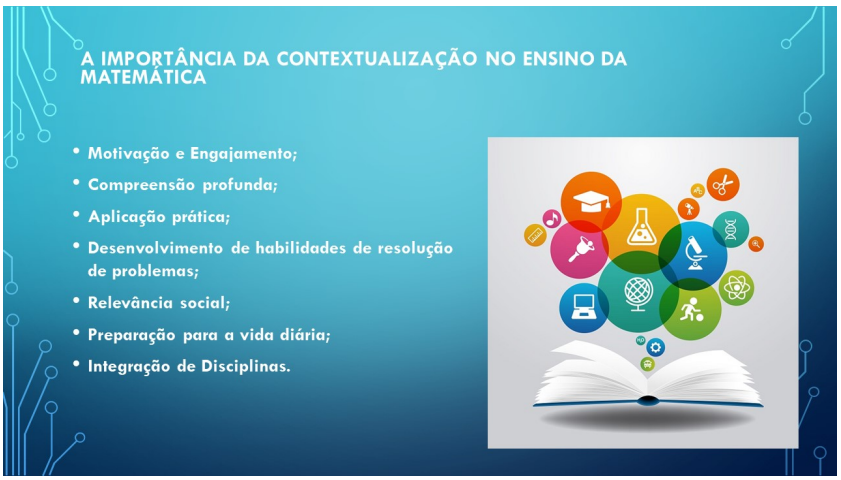

Figura 15: Slide do tópico: A Importância Da Contextualização No Ensino Da Matemática
Fonte: Os Autores (2023)

desse ente matemático está intrínseco na vida das pessoas de forma tão natural, que acaba passando despercebida. Nesse momento, foi utilizado ainda para mencionar que, além do contexto da criptografia, têm-se os exemplos de cinema, telas de modo geral e outros contextos tecnológicos onde as matrizes são amplamente utilizadas.

Dando prosseguimento, no slide seguinte a criptografia foi conceituada como do Grego: Kryptós, "oculto"+ graph, de graphein, "escrever". Foi relatado o seu principal objetivo que é de proteger informações sensíveis e sigilosas. Sua importância não poderia deixar de ser detalhada e por isso foram listados algumas razões pelas quais a criptografia é uma ciência tão importante no mundo atual, como por exemplo sua importância para as comunicações seguras, para a segurança de dados, para a segurança de informações confidenciais, para o comércio eletrônico, entre outras razões. Cada uma das razões apresentadas foi brevemente comentada.

Nos próximos slides foram apresentados alguns tópicos envolvendo a história da criptografia, para uma melhor compreensão do que se trata esta ciência foi comentado que o hábito de guardar informações sob sigilo não é uma prática recente, mas que na verdade vem sendo feita há muito tempo. No Antigo Egito, as pessoas já usavam um modelo de escrita que pode ser considerado um tipo de Criptografia: Os Hieróglifos. Neste modelo de proteção de textos, eram usados desenhos para simbolizar letras ou palavras. Animais comuns, utensílios, partes do corpo humano ou corpos completos em disposições específicas, são exemplos de caracteres dessa escrita. Vale ainda ressaltar que para que isso fizesse sentido para aquele povo, as representações escolhidas estavam diretamente ligadas com o dia a dia dos egípcios. Artefatos históricos que são importantes marcos no desenvolvimento da criptografia também

Figura 16: Slide do tópico: O que é Criptografia?
Fonte: Os Autores (2023)

foram ponteados: A pedra de Roseta - Registro preservado em pedra de escritas em hieróglifos - e o bastão de Licurgo - ferramenta usada para criptografar e descriptografar mensagens normalmente militares e que tinha como chave a largura do bastão.

Figura 17: Slide do tópico: Informações Históricas
Fonte: Os Autores (2023)

Prosseguindo em cunho histórico, foi pontuado um dos tipos mais comuns e memoráveis de criptografia: A cifra de César. Esse modelo de criptografia romana credita sua criação e desenvolvimento significativo ao grande Imperador Júlio César e por esse motivo, recebe essa nomenclatura. Explanou-se o motivo pelo qual esse método foi desenvolvido e também o porquê de ele passar a ser considerado um método obsoleto de proteção de informações. Considerando ainda que, mesmo que tenha caído em desuso, essa forma de criptografia tem

o seu lugar de importância resguardado pelos historiadores que se aprofundam por essa área do conhecimento. Neste próximo momento da narrativa, foi feita alusão ao ponto da história mais marcante para essa ciência: Alan Turing. Circundado de um grupo de criptógrafos experientes, chefiou um grupo de estudos com objetivo militar de interceptar informações militares Alemãs. Como resultado dessa pesquisa, foi criada a Máquina de Turing que é considerada ancestral do computador.

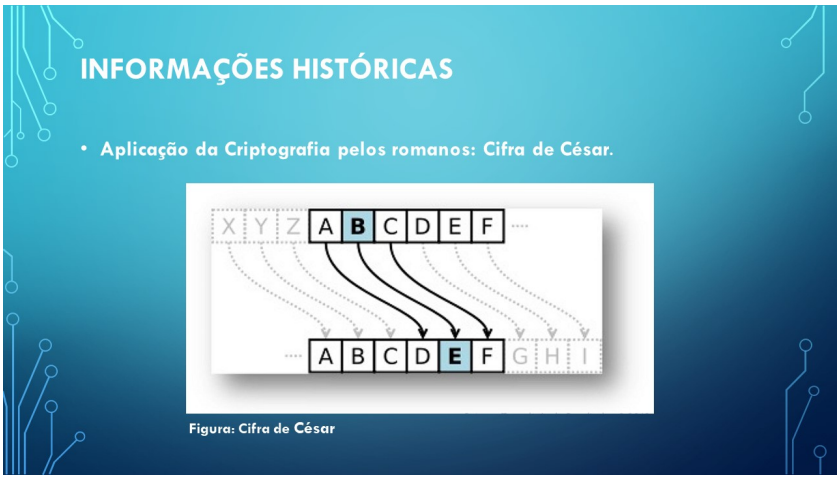

Figura 18: Slide do tópico: Cifra de César
Fonte: Os Autores (2023)

Figura 19: Slide do tópico: Informações Históricas
Fonte: Os Autores (2023)

Foram apontados ainda, os dois tipos de Criptografia: Simétrica (que é o método onde

a chave/algoritmo de criptografia é secreto e a mesma chave é usada tanto para cifrar quanto para decifrar os dados) e Assimétrica, que funciona com uma chave pública e outra privada, onde a chave pública é usada para cifrar os dados, enquanto que a chave privada é usada para decifrar.

Figura 20: Slide do tópico: Criptografia Simétrica
Fonte: Os Autores (2023)

Figura 21: Slide do tópico: Criptografia Assimétrica
Fonte: Os Autores (2023)

Nesse momento, a palestra chegou em seu ponto central: A Cifra de Hill. Desde a elaboração inicial dos tópicos desse trabalho de conclusão de curso, foi vislumbrado que este método seria o ponto central da presente abordagem, uma vez que é um tipo de Criptografia

que se encaixa de forma eficaz na grade curricular comum das escolas brasileiras de Ensino Médio no que se refere ao estudo de matrizes.

Durante a apresentação da Cifra de Hill aos ouvintes, foi mostrado a sua relação com o conteúdo de matrizes e que, portanto, a base matemática para a execução deste algoritmo é ministrada nas instituições de Ensino Médio. Foi mostrado ainda que tendo essa base matemática bem fundamentada, o método de cifragem mencionado já é totalmente passível de compreensão.

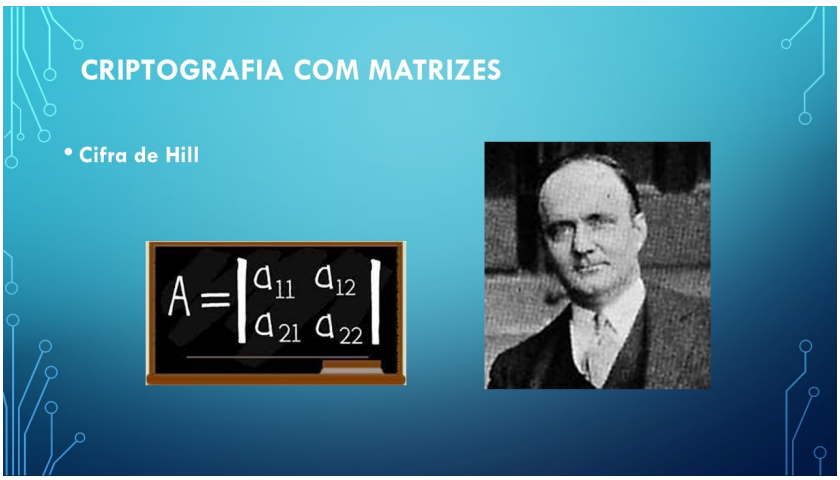

Figura 22: Slide do tópico: Cifra de Hill
Fonte: Os Autores (2023)

A fim de realizar uma demonstração do que seria a Cifra de Hill e fomentar a curiosidade dos ouvintes, foi desenvolvido um exemplo prático de cifragem de uma palavra condizente com o contexto utilizando o algoritmo proposto. A palavra escolhida foi "matemática". Foram evidenciados cada um dos passos, que por sua vez, foram desenvolvidos de forma sistematizada e organizada.

No primeiro passo, foi utilizada uma tabela onde cada letra do alfabeto era representada por um número e foi explicado que essa tabela deveria ser utilizada para que as letras da mensagem fossem previamente cifradas, trocando cada letra da mensagem pelo seu número representante na tabela.

No segundo passo, uma matriz chave de ordem dois foi escolhida e destacado que para a execução deste algoritmo, a chave necessariamente deveria ser uma matriz quadrada e que para fins de simplificação, foi escolhida uma matriz 2x2.

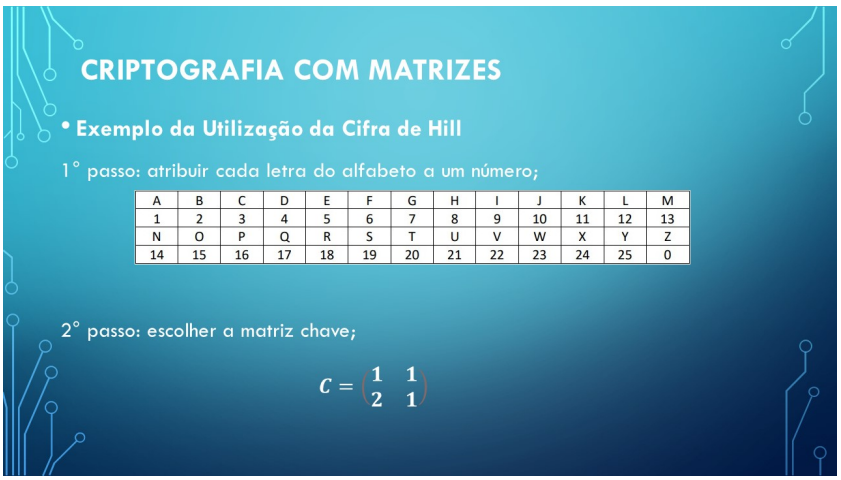

Figura 23: Slide dos Passos 1 e 2
Fonte: Os Autores (2023)

No terceiro passo a palavra cifrada foi divida em blocos de 2 letras e explicado que um pré requisito do método é que o número de letras que cada bloco deve conter, precisa ser igual ao número da ordem da matriz. Ainda nesse passo, as letras do texto a ser cifrado já foram organizadas nos blocos realizando as respectivas transformações, cada letra da mensagem foi trocada pelo seu número correspondente na tabela apresentada no passo 1.

No quarto passo, cada bloco de 2 números foi escrito em vetor coluna uma vez que, visa a multiplicação da matriz chave de criptografia por cada uma das matrizes-coluna gerada pelos blocos do texto original.

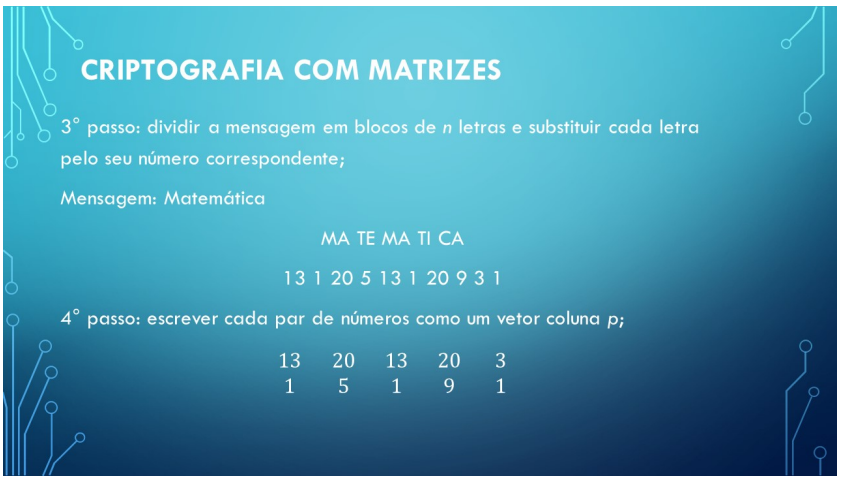

Figura 24: Slide dos Passos 3 e 4
Fonte: Os Autores (2023)

No quinto passo, foi introduzido o raciocínio de módulo (26) uma vez que, a multiplicação dessas matrizes deve resultar em valor qualquer mas que deve ser espelhado dentro do módulo (26) pois é a quantidade de letras que possui o alfabeto brasileiro.

No sexto passo, os valores resultantes da multiplicação das matrizes chave e coluna - já com os valores correspondentes no módulo (26) - são substituídos pelas letras correspondentes no alfabeto da tabela do passo 1. Tendo por sua vez, que o texto MATEMÁTICA cifrado na matriz chave escolhida ficou NAYSNACWDG.

Com o objetivo de despertar a curiosidade do público presente, a demonstração se encerra neste ponto com a promessa que a descriptografia desse texto seria feita no próximo encontro no Laboratório de Informática da UEMASUL.

Figura 25: Slide do Passo 5
Fonte: Os Autores (2023)

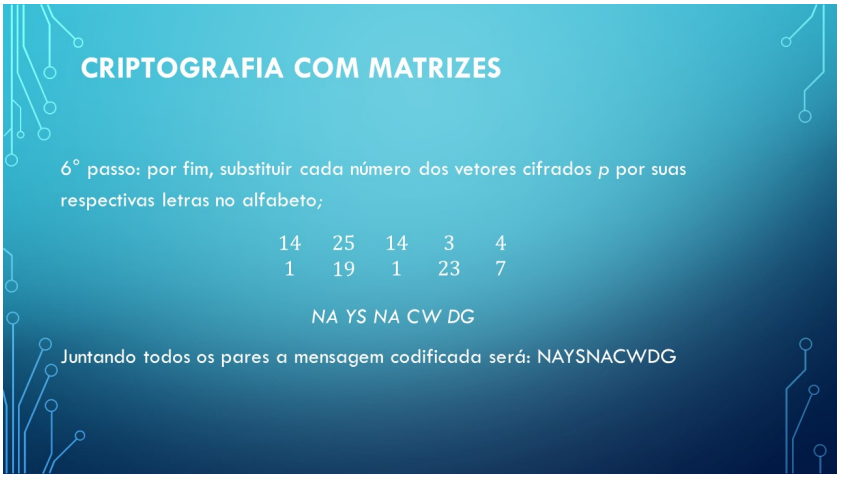

Figura 26: Slide do Passo 6
Fonte: Os Autores (2023)

A palestra encerra, então, com os agradecimentos dos palestrantes à instituição de ensino que prontamente aceitou participar deste trabalho, aos alunos pela atenção e participação durante a apresentação e à professora Gardenia que esteve presente acompanhando os alunos e que cedeu seus horários para a realização da palestra. Logo após os agradecimentos, foram entregues os questionários (anexo tal) aos alunos e à professora presente com o propósito de avaliação do desenvolvimento da palestra.

Figura 27: Participantes da Palestra
Fonte: Os Autores (2023)

4.2 Aula Prática no Laboratório de Informática

4.2.1 Planejamento da aula

Após a realização da palestra, iniciou-se o planejamento da aula que aconteceu na semana seguinte no laboratório de informática da UEMASUL.

4.2.2 Momento prático

Na semana seguinte a realização da palestra, ocorreu a segunda parte da aplicação dessa empreitada pedagógica: levar a turma de alunos para o Laboratório de informática da UEMASUL para a realização da aula onde eles estariam atuando como criptógrafos de forma prática

e absorvendo o conteúdo de maneira mais didática e visual. Todos os preparativos para a aula foram planejados com antecedência, foi verificado se a quantidade de cadeiras disponíveis no laboratório era suficiente para a quantidade de alunos da turma, os computadores já foram todos previamente conectados o GeoGebra, entre outros preparativos. Ao chegarem na Uemasul, os alunos foram recepcionados pelos autores deste trabalho na portaria da instituição e guiados até o laboratório de informática. Durante o percurso, os alunos puderam visualizar algumas das dependências do prédio e mostraram-se entusiasmados com o que estavam vendo. Ao entrar no Laboratório de informática da faculdade, os alunos estavam naturalmente inquietos e apesar de o local já ter passado por uma organização prévia com cadeiras pré dispostas, computadores ligados e com o Software pré carregado, acomodá-los devidamente custou alguns minutos.

Ao tomar posse da palavra, com todos os ouvintes acomodados, os ministrantes da aula oficialmente deram boas vindas a todos, externando gratidão, felicidade e suas expectativas positivas para aquela reunião. A aula foi iniciada fazendo uma breve retomada do que aconteceu no último encontro, momento necessário, uma vez que se tratava de um contexto sequencial que possuía por antecessor um evento ocorrido 7 dias antes. Esta dita revisão se deu inicialmente com breves comentários sobre o que aconteceu no primeiro encontro. Decidiu-se por comentar sobre os tópicos da palestra pois havia alunos que participariam da aula e que não puderam estar presentes no primeiro encontro. Esse primeiro momento foi prosseguido da apresentação de um slide com a definições a respeito de matrizes e, demonstrações genéricas de operações matriciais necessárias para o desenvolvimento do método de Hill.

Após comentar sobre a base matemática necessária para a compreensão da Cifra de Hill e adentrando propriamente ao procedimento de cifragem para fins de exemplificação, o conteúdo específico foi estreado com a proposta de uma chave de criptografia de ordem dois por dois. Vale ainda lembrar que, apesar de ter como um objetivo mostrar que o Software Geogebra seria um facilitador de todo esse procedimento, é importante que os alunos conheçam a realização do procedimento manualmente para que tenham uma noção comparativa, para isso era necessário que os primeiros exemplos fossem feitos de modo tradicional, isto é, através do quadro branco e do pincel. Foi reiterado ainda, o sentido primordial da criptografia que é o de proteger informações sensíveis, confidenciais e afins. Tomando isso por pressuposto, para que o primeiro exemplo fizesse sentido, foi narrado para os alunos um contexto fictício onde um suposto rapaz que, em época que antecedia a internet, necessitava declarar o seu amor por uma moça a quem não possuía acesso direto, e na tentativa de evitar o acesso ao conteúdo da mensagem em caso de interceptação do bilhete, realizou a cifragem da mensagem utilizando

a Cifra de Hill e enviou-o com o texto "OPVK"e uma matriz C = $\begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix}$.

Com isso, foi incentivada a curiosidade e promovida a imaginação lúdica dos ouvintes, e portanto, os cálculos deixaram de ser o vilão da história e se tornaram um aliado para o desvendamento do caso uma vez que, estavam motivados pela história intrigante. Através do simples contexto narrado, foi aberta a oportunidade para revisar e aplicar os conceitos matriciais correlacionados com o método de cifragem. Iniciou-se, então, o processo de decifração da mensagem enviada pelo rapaz e, após discorrer no quadro os cálculos necessários para voltar a mensagem ao seu texto original, utilizando a chave enviada juntamente com a mensagem, foi solucionado que o texto enviado era na verdade, a palavra AMOR. Após resolver essa simples decifração pelo meio tradicional, foi observado que os cálculos feitos a mão se desenvolveram aproximadamente em quarenta minutos.

Prosseguindo com as demonstrações e agora usando um contexto militar, foi exposto um exemplo que trazia o sentido de Pactos Militares. Por ser uma informação mais sigilosa e comprometedora, foi escolhida como chave de criptografia uma matriz de ordem três para dificultar um pouco mais os cálculos. Tendo por base o exemplo anterior, foi conjecturado quanto tempo levaria para desenvolver a palavra PACTOS utilizando a chave D = $\begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 1 \\ 6 & 4 & 2 \end{pmatrix}$.

Foi de comum acordo que o tempo disponível não seria suficiente e, portanto, neste exemplo já seria utilizada a ferramenta facilitadora. Nesse primeiro momento de utilização da plataforma GeoGebra, foi necessário realizar uma breve explicação do que se trata esta ferramenta e, como ela pode ser facilitadora no processo de aprendizagem de diversos conteúdos matemáticos. Introduziu-se, então, o Software na aula e juntamente com os alunos, divididos em duplas com cada dupla em um computador, realizou-se a cifragem e decifragem da palavra PACTOS. Com a ajuda dos autores deste trabalho, os alunos aprenderam a como introduzir uma matriz no GeoGebra, como calcular o determinante da matriz inserida e, no caso do determinante ser diferente de zero, como calcular a inversa dessa matriz além de como realizar multiplicação de matrizes na ferramenta utilizada. Ao observar a facilidade em que todo o cálculo era discorrido, os alunos perceberam a importância e a eficiência do Geogebra.

Após o exemplo militar, foi relembrado que no final da palestra realizada no primeiro encontro foi deixado a palavra MATEMÁTICA criptografada na chave C = $\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$ que teve

como resultado o termo NAYSNACWDG. Neste momento, a descriptografia desse termo foi desenvolvida em conjunto total com os alunos, que mais uma vez tiveram a experiencia de dar as entradas na Plataforma sendo acompanhados e corrigidos pelos palestrantes e auxiliares.

Dando prosseguimento, tendo por objetivo a fixação do conteúdo, foi desenvolvido em sala um exercício onde o texto a ser cifrado e decifrado foi escolhido pelos palestrantes e a chave de encriptação seria escolhida pelos alunos. O exercício foi desenvolvido totalmente em sala de aula, e os alunos puderam perceber que os exemplos apresentados anteriormente não eram palavras isoladas, que funcionavam dentro daquele algoritmo mas que a Cifra de Hill é realmente abrangente e aplicável. A palavra escolhida para o exercício foi CASA e a chave escolhida pelos alunos foi a matriz $\begin{pmatrix} 4 & 1 \\ 2 & -1 \end{pmatrix}$.

Ao final, foi distribuído um questionário bem direcionado e de repostas abertas, isso é, subjetivas, com o objetivo de que os alunos discorressem a respeito da aplicação pedagógica de forma geral. Os questionamentos traziam em seus sentidos aspectos relacionados a interface do software (intuitividade, acessibilidade, funcionalidade e interatividade com o conteúdo); a proposta pedagógica tecnológica (níveis de aplicação, adaptação a outros conteúdos matemáticos, capacidade de engajamento e fixação de atenção); a proposta pedagógica específica da criptografia como meio de ensinar matrizes; o conteúdo e a qualidade do material.

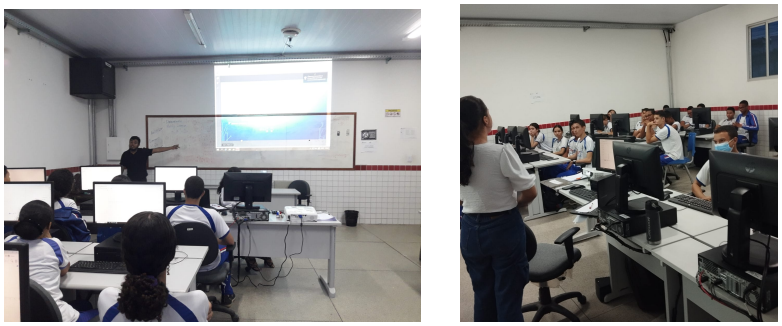

Figura 28: Palestrantes Emersson e Mizia
Fonte: Os Autores (2023)

Figura 29: Participantes da aula
Fonte: Os Autores (2023)

4.3 Nuvem de Palavras

4.3.1 Palestra

No presente tópico será analisada uma nuvem de palavras que foi gerada a partir das respostas ao questionário entregue aos alunos ao final da palestra. Tal questionário continha algumas questões relacionadas ao encontro no que se refere ao nível de satisfação dos estudantes com o conteúdo abordado e a forma como foi abordado. Os ouvintes puderam realizar avaliações a respeito da introdução da palestra e qual o seu desempenho em termos de envolvimento e interesse, tiveram a oportunidade de opinar a respeito dos tópicos abordados na palestra e manifestar o nível de compreensão que obtiveram do assunto além de poderem exprimir suas opiniões a respeito da proposta da Cifra de Hill como aplicação para o aprofundamento do conteúdo de matrizes.

Mediante o recolhimento dos formulários, foram feitas análises sobre o nível de satisfação dos ouvintes ali presentes no que diz respeito a palestra. Posteriormente, todas as informações foram digitadas e processadas na plataforma R-Studio com o objetivo de serem analisadas estatisticamente através da ferramenta chamada de nuvem de palavras. Essa por sua vez, possui por objetivo disponibilizar, através dos dados informados, uma análise qualitativa e quantitativa de fácil compreensão uma vez que analisa textos subjetivos fazendo com que as opiniões individuais, independentemente da quantidade, tenha lugar reservado no gráfico final. Quanto a análise quantitativa da suposta opinião, se dá através do destaque que os termos são evidenciados.

Como resultante do conjunto de informações que foram processadas desse questionário, foi obtido o gráfico evidenciado na Figura 35.

Figura 30: Nuvem de Palavras da Palestra
Fonte: Os Autores (2023)

A nuvem de palavras resultante desse questionário apresenta uma variedade de termos relacionados ao tema, como "Cifra de Hill", "Matrizes", "Compreender", "Criptografia", "Aplicação", entre outras evidentes na imagem. As palavras em destaque, que aparecem em um tamanho maior, são as palavras que apareceram com mais frequência nas respostas dos alunos.

Observa-se que os termos mais proeminentes na nuvem de palavras estão relacionados à compreensão do conteúdo abordado e sua importância. Os resultados sugerem que os ouvintes ali presentes internalizaram o objetivo principal deste trabalho que é o de perceber que a abordagem torna melhor a compreensão do assunto de matrizes através do processo de criptografia que se utiliza do método da Cifra de Hill. Ademais, podemos extrair que a aplicação foi vista de forma satisfatória pois diversos termos positivos se encontram em destaque. Diante do exposto, cabe considerar que os alunos saíram da palestra motivados a irem ao próximo nível da proposta, que é o de ver na prática se todo esse pressuposto é de fato aplicável, dinâmico e motivador quanto foi passado pelos palestrantes.

4.3.2 Aula Prática

Após a conclusão do momento prático, os participantes responderam um questionário subjetivo que tinha como objetivo observar alguns itens a respeito da aplicação pedagógica. Os questionamentos eram direcionados a aspectos como a interface do software (intuitividade, acessibilidade, funcionalidade e interatividade com o conteúdo); a proposta pedagógica tecnológica (níveis de aplicação, adaptação a outros conteúdos matemáticos, capacidade de engajamento e fixação de atenção); a proposta pedagógica específica da criptografia como meio de ensinar matrizes, o conteúdo e a qualidade do material.

Como gráfico resultante, observa-se a Figura 36:

Figura 31: Nuvens de Palavras da Aula
Fonte: Os Autores (2023)

Partindo do mesmo princípio de análise já discorrido anteriormente, pode-se observar que como resultado, foi obtida uma turma com um bom aproveitamento do conteúdo ministrado pois o gráfico evidencia que o Software Geogebra com toda a sua interface intuitiva e dinâmica, torna a proposta de aprendizagem do conteúdo bem facilitada, uma vez que torna o processo de ensino-aprendizagem mais atraente pois possibilita estudar matrizes de forma contextualizada e interessante. Além do mais, o recurso utilizado propicia compreensão de maneira geral, uma vez que se trata de um facilitador de cálculos e, portanto, pode ser apli-

cado em outras áreas do conhecimento matemático.

4.4 Análise de Sentimentos

A técnica de análise de sentimentos, também conhecida como mineração de opiniões, é utilizada neste trabalho para a compreensão das emoções e opiniões expressas nos questionários aplicados aos alunos após a palestra e a aula sobre criptografia. Seu objetivo principal é identificar e compreender as características sentimentais dos discentes ao analisar suas opiniões sobre a proposta pedagógica apresentada. Essa abordagem é aplicada por meio de métodos que examinam os elementos textuais e os comparam com padrões emocionais predefinidos, conforme descrito por autores como Raji e Zainal (2016).

A importância da análise de sentimentos reside na capacidade de compreender a percepção dos discentes sobre a proposta elaborada neste trabalho. Empresas e pesquisadores dedicam esforços para desenvolver ferramentas computacionais capazes de identificar a subjetividade humana em textos originados em diversos contextos, como redes sociais, sites de avaliações de produtos e serviços, fóruns de discussões, entre outros. Isso é particularmente relevante, pois muitas empresas já aplicam a análise de sentimentos para identificar aspectos emocionais e subjetivos de cada cliente.

Ao compreender as opiniões e emoções expressas pelos discentes, pode-se avaliar se as estratégias pedagógicas foram alinhadas com os objetivos da pesquisa, possibilitando oferecer um melhor feedback, comparando a teoria com as expectativas geradas pelos discentes. Esse entendimento aprofundado das preferências e sentimentos dos discentes permite que através da pesquisa as instituições de ensino possam tomar decisões sobre suas metodologias de ensino e personalizar suas ofertas, melhorando assim a satisfação da sociedade fortalecendo a relação entre escola e sociedade, conforme destacado por De Castro e Ferrari (2017).

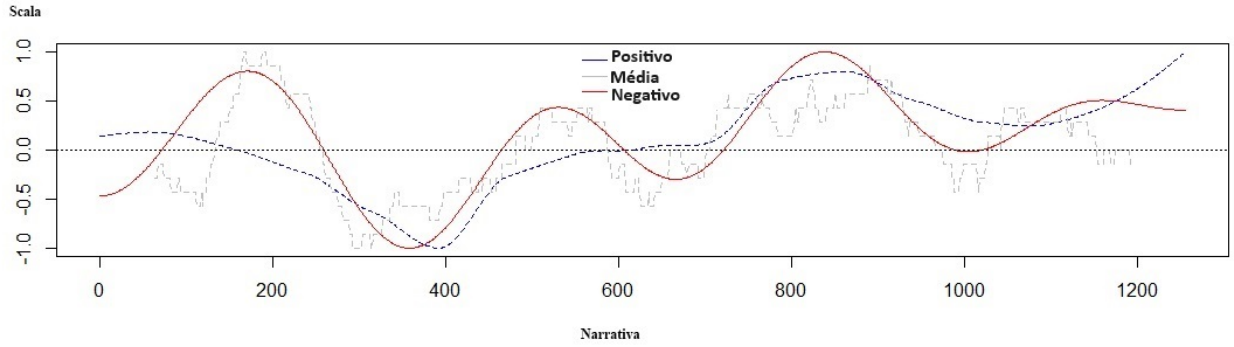

Figura 32: Análise de Sentimento referente aos questionários aplicados aos alunos
Fonte: Os Autores (2024)

Os dados remetem diretamente às representações sociais construídas no espaço da sala de aula, pois implicam na forma como o discente vivencia o aprendizado do conteúdo de matrizes no seu percurso escolar. Se o discente vivencia uma experiência inovadora de apresentação do conteúdo, isto propicia uma construção representativa positiva. O gráfico mostra que no início há uma expectativa positiva sobre o conhecimento de uma nova proposta pedagógica relativa ao ensino de matrizes, porém os relatos iniciais dos discentes levam a crer que existe um pessimismo sobre o desenvolvimento de novas propostas, pois elas acabam retornando ao processo clássico de aprendizado. Após o término do processo pedagógico proposto nesta pesquisa os discentes se apresentam mais otimistas e motivados a aprender o conteúdo de matrizes. No final da análise o gráfico apresenta uma representação positiva das expectativas dos discentes. A maior parte dos discentes, ao falar sobre sua relação com o aprendizado do conteúdo de matrizes, afirma que a forma tradicional não oportuniza a visualização de aplicação prática do mesmo. Entende-se esse dado como um distanciamento desse grupo com o aprender, pois esses discentes não conseguem se vincular aos conteúdos, porque apresentam dificuldades, e nem com seu professor, em razão da sua própria conduta de ensinar a matemática de forma clássica.

5 CONSIDERAÇÕES FINAIS

Esse trabalho, se deu através da aplicação da Criptografia - mais precisamente da Cifra de Hill - como abordagem pedagógica para o ensino de matrizes. Ao findar dessa jornada, o que se considera como desfecho de todo o processo, é que a criptografia pode servir como um recurso motivador e prático para engajar os alunos no aprendizado de conceitos matriciais, proporcionando uma compreensão mais profunda dos fundamentos matemáticos envolvidos.

Neste método utilizado, conceitos matemáticos como multiplicação de matrizes; cálculo de determinante; Matriz inversa e noção de módulo, demonstram como cada definição aqui citada pode ser aplicada de forma prática, concreta e contextualizada. Supõe-se que a consequência dessa aplicação, serão aprendizes com conhecimentos mais sólidos, uma vez que valorizarão o processo e estarão mais cientes e seguros de seus resultados tornando-se assim, futuros profissionais mais críticos e capazes diante dos desafios do mercado de trabalho.

Além disso, cabe considerar, que a criptografia oferece potenciais vantagens se for usada como ferramenta educacional, uma vez que inclui para o discente o desenvolvimento de habilidades como pensamento crítico, resolução de problemas, trabalho em equipe, contato e familiarização com a tecnologia, dentre outras. Cabe ainda ressaltar, que este mesmo beneficiado, provavelmente sairá da sala de aula mais preparado para enfrentar os desafios do mundo digital contemporâneo e ainda ciente a respeito dos temas de segurança cibernética e privacidade de dados. Por outro ângulo, o que pressupõe-se para o docente é que o mesmo obterá mais satisfação e realização profissional uma vez que, o conteúdo ministrado será bem mais absorvido pelos seus aprendizes e suas aulas serão cada vez mais dinâmicas, didáticas, tecnológicas, motivadoras e afins.

Para tanto, para que essa abordagem pedagógica venha a lograr êxito em sua aplicação prática nas escolas brasileiras, se faz necessário não apenas materiais de qualidade e a metologia aqui apresentada, mas também é de suma importância o apoio geral das autoridades maiorais do Estado e a capacitação adequada para os ministrantes. Portanto, recomenda-se investimentos contínuos em formação de professores e na disponibilização de recursos educacionais.

Por decorrência de todos os argumentos apresentados, considera-se que a integração da criptografia aplicada como uma ferramenta prática e facilitadora do ensino de matrizes, pode representar uma empolgante oportunidade para enriquecer o currículo escolar. Além de ser um

possível incentivo para o interesse dos alunos pela Matemática e pela Ciência da Computação. Por desfecho, o que se espera desse trabalho é que o mesmo sirva de inspiração para novas abordagens pedagógicas e que possa contribuir para o avanço da Educação das Ciências Exatas e Tecnológicas.

REFERÊNCIAS

ALMEIDA, P. J.; NAPP, D. Criptografia e segurança. **Departamento de Matemática da Universidade de Aveiro**, 2012.

ANA, W. P. S.; LEMOS, G. C. Metodologia Científica: a pesquisa qualitativa nas visões de lüdke e andré. **Revista Eletrônica Científica Ensino Interdisciplinar**, v. 4, n. 12, 2018.

ANDRADE, R. S.; SANTOS SILVA, F. dos. Algoritmo de criptografia RSA: análise entre a segurança e velocidade. **Revista Eventos Pedagógicos**, v. 3, n. 3, p. 438–457, 2012.

ANTON, H.; BUSBY, R. C. **Álgebra linear contemporânea**. Bookman Editora, 2006.

BARBOSA, L. A. d. M.; BRAGHETTO, L. F. B.; BRISQUI, M. L.; SILVA, S. C. da. RSA Criptografia Assimétrica e Assinatura Digital. **Especialização em Redes de Computadores. Universidade Estadual de Campinas**, 2003.

BARRETO, P. S.; BIASI, F. P.; DAHAB, R.; LÓPEZ-HÉRNANDEZ, J. C.; MORAIS, E.; OLIVEIRA, A. D. S. de; PEREIRA, G. C.; RICARDINI, J. E. Introdução à criptografia pós-quântica. **Sociedade Brasileira de Computação**, 2013.

BOLDRINI, J. L.; COSTA, S. I.; FIGUEREDO, V.; WETZLER, H. G. **Álgebra linear**. Harper & Row, 1980.

CARVALHO, A. L.; RODRIGUES, D. V.; ARAÚJO, L. H. R. et al. Aplicações da aritmética modular na criptografia. **Caderno de Graduação-Ciências Exatas e Tecnológicas-UNIT-SERGIPE**, v. 3, n. 1, p. 11–24, 2015.

CORDEIRO, N. V. et al. Certificação digital. , 2011.

DE CASTRO, L. N.; FERRARI, D. G. **Introdução à mineração de dados**. Saraiva Educação SA, 2017.

FEDERAL, S. Lei de diretrizes e bases da educação nacional. , 2005.

FIARRESGA, V. M. C. et al. **Criptografia e matemática**. 2010. Tese , 2010.

GOMES, A. S.; CASTRO FILHO, J. A.; GITIRANA, V.; SPINILLO, A.; ALVES, M.; MELO, M.; XIMENES, J. Avaliação de software educativo para o ensino de matemática. In: WIE 2002 WORKSHOP BRASILEIRO DE INFORMÁTICA EDUCATIVA. FLORIANÓPOLIS: SBC, 2002. **Anais...** 2002.

GROENWALD, C.; OLGIN, C. Códigos e senhas: sequência didática com o tema criptografia no ensino fundamental. **X Encontro Nacional de Educação Matemática**, 2010.

JESUS BRITO, A. de; LITOLDO, B. F. CONHECENDO E PRATICANDO: a criptografia dentro da sala de aula. **Sociedade Brasileira de Educação Matemática - São Paulo**, 2016.

LAUDARES, J. B.; LACHINI, J. O uso do computador no ensino de matemática na graduação. **23a Reunião Anual da Associação Nacional de Pós-Graduação e Pesquisa em Educação**, p. 32–43, 2000.

LIPSCHUTZ, S.; LIPSON, M. L. **Álgebra linear**. Bookman, 2011.

MACHADO, C. P. **Investigando o uso de softwares educacionais como apoio ao ensino de Matemática**. 2011. Dissertação Pontifícia Universidade Católica do Rio Grande do Sul, 2011.

MENEZES, E. d. Fundamentos sociológicos da comunicação. **Fundamentos científicos da comunicação. Petrópolis: Vozes**, p. 145–205, 1973.

MORAIS, F.; NORONHA, I. UMA ABORDAGEM HISTÓRICA, EVOLUTIVA E APLICACIONAL DA CRIPTOGRAFIA. , 2014.

MOREIRA, A. F. B. Os parâmetros curriculares nacionais em questão. **Educação & Realidade**, v. 21, n. 1, 1996.

NASCIMENTO, F. P. d.; SOUSA, F. Classificação da Pesquisa. Natureza, método ou abordagem metodológica, objetivos e procedimentos. **Metodologia da Pesquisa Científica: teoria e prática–como elaborar TCC. Brasília: Thesaurus**, 2016.

PONTES, E. A. S. HIPERMAT–Hipertexto Matemático: uma ferramenta no ensino-aprendizagem da matemática na educação básica. **Revista Psicologia & Saberes**, v. 2, n. 2, 2013.

PONTES, E. A. S. O ato de ensinar do professor de matemática na educação básica. **Ensaios Pedagógicos**, v. 2, n. 2, p. 109–115, 2018.

PORTO, V. M. F. et al. Criptografia: da origem aos dias atuais. , 2015.

QUARESMA, P.; LOPES, E. 2 O Surgimento da Criptografia. .

RAJI, M. N. A.; ZAINAL, A. The effect of customer perceived value on customer satisfaction: a case study of malay upscale restaurants. **Geografia**, v. 12, n. 3, 2016.

SILVA, W. et al. A Evolução da Criptografia e Suas Técnicas ao Longo da História. , 2019.

SILVEIRA, A. S. d.; FALEIROS, A. C. Criptografia de chave pública–O papel da aritmética em precisão múltipla. **ENCONTRO DE INICIAÇÃO CIENTÍFICA E PÓS-GRADUAÇÃO DO ITA**, v. 11, 2005.

SIQUEIRA, A. C.; JUNIOR, V. S.; LAHM, R. A.; VIALI, L. Tecnologias no ensino de matemática: recursos e possibilidades do software scilab para o ensino de matrizes. **REVISTA CIÊNCIAS & IDÉIAS**, 2020.

APÊNDICE A QUESTIONÁRIOS APLICADOS

UNIVERSIDADE ESTADUAL DA REGIÃO TOCANTINA DO MARANHÃO – UEMASUL
MATEMÁTICA LICENCIATURA
CRIPTOGRAFIA E MATEMÁTICA: PROTEGENDO INFORMAÇÕES COM MATRIZES
ACADÊMICOS: EMERSSON SILVA DA LUZ E MIZIA SILVA LIMA
ORIENTADOR: PROF. DR. MURILO BARROS ALVES

QUESTIONÁRIO DE AVALIAÇÃO DA PALESTRA

1. COMO VOCÊ AVALIARIA A INTRODUÇÃO DA PALESTRA EM TERMOS DE ENVOLVIMENTO E INTERESSE?

   ( ) BOM ( ) MEDIANO ( ) RUIM

2. EM SUA OPINIÃO, A PALESTRA ABORDOU TÓPICOS RELEVANTES PARA A SUA COMPREENSÃO E INTERESSE?

   ( ) SIM ( ) NÃO

3. FOI POSSÍVEL COMPREENDER O QUE É CRIPTOGRAFIA E SUA IMPORTÂNCIA NA SEGURANÇA DA INFORMAÇÃO?

   ( ) SIM ( ) NÃO

4. FOI POSSÍVEL COMPREENDER A IMPORTÂNCIA DA MATEMÁTICA NO MUNDO ATUAL?

   ( ) SIM ( ) NÃO

5. FOI POSSÍVEL COMPREENDER COMO A MATEMÁTICA ESTÁ RELACIONADA COM A CRIPTOGRAFIA?

   ( ) SIM ( ) NÃO

6. FOI POSSÍVEL COMPREENDER COMO AS MATRIZES PODEM SER UTILIZADAS NA CIFRA DE HILL?

   ( ) SIM ( ) NÃO

7. VOCÊ CONSIDERA QUE A CIFRA DE HILL PODE SER UM BOM EXEMPLO DE APLICAÇÃO PARA O APROFUNDAMENTO DO CONTEÚDO DE MATRIZES?

   ( ) SIM ( ) NÃO

8. QUAL O SEU NÍVEL DE SATISFAÇÃO COM A PALESTRA?

   ( ) MUITO SATISFEITO ( ) SATISFEITO ( ) POUCO SATISFEITO ( ) NÃO SATISFEITO

9. QUE SUGESTÕES VOCÊ TERIA PARA FUTURAS APRESENTAÇÕES?

   _____

   _____

10. EXISTE ALGUMA ÁREA ESPECÍFICA EM QUE VOCÊ ACHA QUE A PALESTRA PODERIA SER APRIMORADA?

    _____

    _____

UEMASUL
Universidade Estadual
da Região Tocantina
do Maranhão

MATEMÁTICA LICENCIATURA
CRIPTOGRAFIA E MATEMÁTICA: PROTEGENDO INFORMAÇÕES COM MATRIZES
ACADÊMICOS: EMERSSON SILVA DA LUZ E MIZIA SILVA LIMA
ORIENTADOR: PROF. DR. MURILO BARROS ALVES

Questionário sobre a aplicação didática da criptografia no Geogebra

1. **Usabilidade e Interface do Usuário:**
   - Como é a interface do software? É intuitiva?
   - Os recursos e funcionalidades didáticas estão facilmente acessíveis?
   - O software facilita a compreensão e a interação com o conteúdo matemático?
2. **Adaptabilidade e Personalização:**
   - A proposta didática e tecnológica oferece diferentes níveis de aplicação para atender às necessidades de aprendizado dos alunos?
   - É adaptável a diferentes conteúdos matemáticos?
3. **Engajamento e Interatividade:**
   - A proposta tecnológica educacional consegue manter o interesse e a atenção dos alunos?
4. **Feedback e Avaliação:**
   - Como você avalia a proposta da criptografia aplicado ao ensino de matrizes?
   - O geogebra atende e ajuda no melhor entendimento do conteúdo?
5. **Conteúdo e Qualidade do Material:**
   - O material educativo presente no software é relevante, atualizado e preciso?
   - Como é a variedade de conteúdo oferecida?

ANEXO A TERMO DE CONSENTIMENTO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO REFERENTE AS INFORMAÇÕES CEDIDAS PELA ESCOLA MILITAR TIRADENTES (CMT) AOS FORMANDOS MIZIA SILVA LIMA E EMERSSON SILVA DA LUZ SOB ORIENTAÇÃO DO PROF. DR MURILO BARROS ALVES

OBJETIVO DO ESTUDO: INSERIR A ESCOLA MILITAR TIRADENTES NO PROJETO PEDAGÓGICO "CRIPTOGRAFIA: UMA ABORDAGEM PEDAGÓGICA PARA O ESTUDO DE MATRIZES NO ENSINO MÉDIO" QUE TEM POR OBJETIVO O RECOLHIMENTO E A PUBLICAÇÃO DE INFORMAÇÕES NECESSÁRIAS PARA O TRABALHO DE CONCLUSÃO DE CURSO DOS FORMANDOS.

ALTERNATIVA PARA PARTICIPAÇÃO NO ESTUDO: A escola tem o direito de não participar deste estudo.

PROCEDIMENTO DO PROJETO:
- PALESTRA INTRODUTÓRIA COM O TEMA: "PROTEGENDO INFORMAÇÕES COM MATRIZES";
- RECOLHIMENTO DE QUESTIONÁRIO PERTINENTE A ESSE PRIMEIRO ENCONTRO;
- AULA PRÁTICA DE CIFRA DE HILL NO LABORATÓRIO DE INFORMÁTICA DA UEMASUL COM O USO DO SOFTWARE GEOGEBRA COMO FACILITADOR;
- RECOLHIMENTO DE QUESTIONÁRIO PERTINENTE AO ENCONTRO PRÁTICO;

DOCUMENTAÇÃO DO PROJETO: Todas os encontros serão fotografados para geração de documentos que serão posteriormente usados como provas da ocorrência dos eventos e publicados no escopo do Trabalho de Conclusão de Curso (TCC) e anexados ao mesmo. Os autores da pesquisa poderão citar no trabalho o nome da instituição que participou da atividade pedagógica como também o nome dos professores que acompanharam os estudantes para que suas contribuições sejam reconhecidas adequadamente na documentação final.

BENEFÍCIOS: O consentimento do projeto acarretará em benefícios para os formandos uma vez que, darão prosseguimento ao seu TCC. A escola será beneficiada com o oferecimento de uma aplicação pedagógica diferenciada e empolgante para os alunos da casa. E os discentes por sua vez, serão os mais beneficiados pois terão um aprofundamento científico do conteúdo matemático de matrizes feito de forma didática, tecnológica e motivacional.

OBSERVAÇÕES: Esta pesquisa está sendo supervisionada pelo corpo pedagógico da Universidade Estadual da Região Tocantina do Maranhão (UEMASUL) e Orientada pelo Professor Doutor Murilo Barros Alves.

Enquanto escola, concordamos em participar deste estudo. Para firmar o combinado, seguem as seguintes assinaturas:

Aurenir Terto de Sousa

Diretora Pedagógica do Colégio Militar Tiradentes (CMT)

Aurenir Terto de Sousa
Gestora Auxiliar-CMT II (SEDUC)
MAT: 297296-03

José Alves Feliciano da Silva

Professor de Matemática

Jacqueline Vieira Costa

Professora de Matemática

Orientador

Mirja Silva Lima

Formando 1

Emersson Silva da Luz

Formando 2

06 de Novembro de 2023

Imperatriz - Ma