

UNIVERSIDADE FEDERAL DO PAMPA

LÚCIA ADRIANA GUDAITES

A CRIPTOGRAFIA COMO TEMA MOTIVADOR PARA O ENSINO DE MATRIZES

**Bagé
2023**

LÚCIA ADRIANA GUDAITES

A CRIPTOGRAFIA COMO TEMA MOTIVADOR PARA O ENSINO DE MATRIZES

Trabalho de Conclusão de Curso apresentado ao Curso de Especialização em Ensino de Matemática no Ensino Médio: Matemática na Prática da Universidade Federal do Pampa, na modalidade EaD - Pólo Gravataí como requisito parcial para obtenção do certificado de Especialista em Ensino de Matemática para o Ensino Médio.

Orientadora: Profa. Dra. Francieli Aparecida Vaz

Coorientador: Prof. Dr. Leandro Blass

**Bagé
2023**

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais).

G922c Gudaites, Lúcia Adriana

A criptografia como tema motivador para
o ensino de matrizes / Lúcia Adriana
Gudaites.

100 p.

Trabalho de Conclusão de Curso (Especialização) --
Universidade Federal do Pampa, ESPECIALIZAÇÃO EM
MATEMÁTICA NO ENSINO MÉDIO (MATEMÁTICA NA PRÁTICA),
2023.

"Orientação: Francieli Aparecida Vaz".

1. Criptografia. 2. Matemática. 3. Motivação. 4.
Ensino. 5. Matrizes. I. Título.

LÚCIA ADRIANA GUDAITES

A CRIPTOGRAFIA COMO TEMA MOTIVADOR PARA O ENSINO DE MATRIZES

Trabalho de Conclusão de Curso apresentado ao Curso de Especialização em Ensino de Matemática no Ensino Médio: Matemática na Prática da Universidade Federal do Pampa, na modalidade EaD - Pólo Gravataí como requisito parcial para obtenção do certificado de Especialista em Ensino de Matemática para o Ensino Médio.

Trabalho de Conclusão de Curso defendido e aprovado em: 25/01/23.

Banca examinadora:

Prof. Dra. Francieli Aparecida Vaz

Orientadora

UNIPAMPA

Prof. Dr. Anderson Luís Jeske Bihain

UNIPAMPA

Prof. Dr. Cristiano Peres Oliveira

UNIPAMPA



Assinado eletronicamente por **FRANCIELI APARECIDA VAZ, PROFESSOR DO MAGISTERIO SUPERIOR**, em 07/02/2023, às 08:29, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.



Assinado eletronicamente por **CRISTIANO PERES OLIVEIRA, PROFESSOR DO MAGISTERIO SUPERIOR**, em 07/02/2023, às 11:47, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.



Assinado eletronicamente por **ANDERSON LUIS JESKE BIHAIN, PROFESSOR DO MAGISTERIO SUPERIOR**, em 08/02/2023, às 11:29, conforme horário oficial de Brasília, de acordo com as normativas legais aplicáveis.



A autenticidade deste documento pode ser conferida no site https://sei.unipampa.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1047940** e o código CRC **70A6322F**.

“Dedico este trabalho aos meus filhos, minha razão de viver, e ao meu marido, que deu todo apoio para que eu pudesse desenvolver este projeto.”

AGRADECIMENTOS

À professora orientadora Dra. Francieli Aparecida Vaz, pela atenção dedicada ao longo do meu projeto de monografia e ensinamentos que me possibilitaram um melhor desempenho no meu processo de formação profissional ao longo do curso.

Ao professor coorientador Dr. Leandro Blass, pela atenção dedicada ao meu projeto de monografia e ensinamentos que me possibilitaram um melhor desempenho no meu processo de formação profissional ao longo do curso.

Aos professores, Dr. Anderson Luís Bihain, Dr. Cristiano Peres Oliveira e Dr. Everson Jonatha Gomes da Silva, pelos ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso.

À professora tutora Ana Patrícia Sampaio, pela sua atenção dedicada ao longo do curso.

A todos os meus queridos alunos que participaram deste trabalho.

E a todas as pessoas que, direta ou indiretamente, contribuíram para a realização desta pesquisa.

“O mistério gera curiosidade e a curiosidade é a base do desejo humano para compreender.”

(Neil Armstrong)

RESUMO

A constante desmotivação com a aprendizagem da matemática por parte dos alunos, gera certa frustração no ensino da matemática por parte dos professores. O ensino tradicional, baseado no ensino teórico e expositivo, já não é suficiente para as necessidades escolares, sendo necessários outros métodos de ensino para complementar e motivar a aprendizagem. Pensando nisso, considerou-se a criptografia como tema motivador na aprendizagem de conteúdos matemáticos, por ser um assunto interessante e desafiador, que pode ser utilizado em diversas atividades educacionais. A criptografia faz parte da história da matemática, pois grande parte do desenvolvimento da criptografia se deve à matemática, que estuda e elabora estratégias para tornar a criptografia mais complexa de decifrar. A criptografia usa técnicas que transformam uma mensagem legível em ilegível, de modo que apenas o remetente e o destinatário possam entendê-la, garantindo a confidencialidade das informações associadas à mensagem. Esta investigação qualitativa visa observar, analisar e relatar os resultados obtidos em aplicações que relacionam criptografia e matemática, atribuindo significado ao conceito matemático estudado, destacando assim a importância de trazer para a sala de aula temas atuais que relacionam a matemática com a realidade do aluno, motivando-o a aprender de uma forma agradável e proveitosa. A pesquisa é de natureza exploratória e envolve um levantamento bibliográfico sobre criptografia, seus aspectos históricos e conceitos matemáticos relacionados ao ambiente criptográfico. Para a elaboração dos dados desta pesquisa foram aplicadas propostas didáticas com atividades que usam a matemática, mais especificamente matrizes de segunda e terceira ordem, para criptografar e decifrar mensagens. As atividades foram realizadas por alunos de uma turma de segundo ano do Ensino Médio de uma escola pública estadual, situada na cidade de Esteio, no estado do Rio Grande do Sul. Posteriormente, os alunos responderam a um questionário visando analisar os aspectos benéficos, ou não, dessas aplicações. Destaca-se entre as percepções, após a análise das atividades, que este tema motivou e fez com que a turma reagisse de forma positiva diante da proposta didática. Este estudo pode ser utilizado por professores do Ensino Fundamental e Médio para rever, corrigir, aprofundar e exercitar os conteúdos matemáticos lecionados, podendo ser elaboradas outras versões destas atividades, adaptando-as ao público-alvo, ou usando outras técnicas de encriptação, ou outros conteúdos matemáticos, tornando as aulas de matemática mais atrativas e significativas.

Palavras-chave: Criptografia; Motivação; Aprendizagem; Matemática.

ABSTRACT

The constant lack of motivation with the students' learning of Mathematics generates a certain frustration in the teaching of Mathematics on the part of the teachers. Traditional teaching, based on theoretical and expository teaching, is no longer sufficient for school needs, requiring other teaching methods to complement and motivate learning. With that in mind, cryptography was considered a motivating theme in the learning of mathematical content, as it is an interesting and challenging subject that can be used in various educational activities. Cryptography is part of the history of mathematics, as much of the development of cryptography is due to mathematics, which studies and devises strategies to make cryptography more complex to decipher. Encryption uses techniques that transform a readable message into an unreadable one, so that only the sender and recipient can understand it, ensuring the confidentiality of information associated with the message. This qualitative investigation aims to observe, analyze and report the results obtained in applications that relate cryptography and mathematics, attributing meaning to the mathematical concept studied, thus highlighting the importance of bringing current topics that relate mathematics to the student's reality to the classroom, motivating you to learn in an enjoyable and profitable way. The research is exploratory in nature and involves a bibliographic survey on cryptography, its historical aspects and mathematical concepts related to the cryptographic environment. For the elaboration of the data of this research, didactic proposals were applied with activities that use mathematics, more specifically second and third order matrices, to encrypt and decipher messages. The activities were carried out by students from a second-year high school class at a state public school, located in the city of Esteio, in the state of Rio Grande do Sul. Subsequently, the students answered a questionnaire in order to analyze the beneficial aspects, or not, of these applications. It stands out among the perceptions, after analyzing the activities, that this theme motivated and made the class react positively to the didactic proposal. This study can be used by elementary and high school teachers to review, correct, deepen and exercise the mathematical content taught, and other versions of these activities can be prepared, adapting them to the target audience, or using other encryption techniques, or other mathematical contents, making mathematics classes more attractive and meaningful.

Keywords: Encryption; Motivation; Learning; Math.

LISTA DE FIGURAS

Figura 1 - Bilhete criptografado.....	19
Figura 2 - Páginas do manuscrito Voynich.....	20
Figura 3 - Literatura no Antigo Egito: o Livro dos Mortos.....	21
Figura 4 - Bastão de Licurgo ou Cítala espartana.....	22
Figura 5 - Quadrado de Políbio.....	23
Figura 6 - Imperador romano Júlio César.....	24
Figura 7 - O quadrado da Cifra de Vigenère.....	25
Figura 8 - Primeira página do manuscrito de al-Kindy.....	27
Figura 9 - Gráfico com a frequência das letras em português.....	28
Figura 10 - Máquina Enigma.....	29
Figura 11 - Algoritmo de criptografia.....	30
Figura 12 - Criptografia simétrica.....	30
Figura 13 - Criptografia assimétrica.....	31
Figura 14 - Cenas do vídeo: A César, o que é de César!	58
Figura 15 - La Skytale.....	58
Figura 16 - Cenas do vídeo: O gabarito secreto.....	60
Figura 17 - Mensagem no aplicativo WhatsApp.....	72
Figura 18 - Gráfico 1: quanto ao tema da pesquisa.....	72
Figura 19 - Gráfico 2: respostas à pergunta 2 quanto à utilidade da criptografia.....	73
Figura 20 - Pergunta 2 e suas alternativas.....	73
Figura 21 - Gráfico 3: quanto às técnicas antigas de criptografia.....	74
Figura 22 - Alunas desenvolvendo a atividade 1.....	74
Figura 23 - Gráfico 4: quanto à atividade 1 - A César, o que é de César!	75
Figura 24 - Atividade 2 resolvida por um dos grupos.....	74
Figura 25 - Gráfico 5: respostas da pergunta 5 quanto à atividade 2.....	76
Figura 26 - Pergunta 5 e suas alternativas.....	76
Figura 27 - Alunas comparando a atividade 3.....	78

Figura 28 - Alunas desenvolvendo a atividade 3.....	78
Figura 29 - Atividade 3 resolvida por um dos grupos.....	79
Figura 30 - Gráfico 6: respostas da pergunta 6 quanto à atividade 3.....	79
Figura 31 - Pergunta 6 e suas alternativas.....	80
Figura 32 - Atividade 4 resolvida pelo aluno com detalhe do erro.....	81
Figura 33 - Atividade 4 com detalhe do erro na resposta do aluno.....	81
Figura 34 - Atividade 4 corretamente resolvida pelo aluno.....	82
Figura 35 - Gráfico 7: respostas da pergunta 7 quanto à atividade 4.....	82
Figura 36 - Pergunta 7 e suas alternativas.....	83
Figura 37 - Gráfico 8: respostas da pergunta 8.....	83
Figura 38 - Pergunta 8 e suas alternativas.....	84
Figura 39 - Gráfico 9: quanto a relacionar matemática a outros assuntos.....	84
Figura 40 - Gráfico 10: quanto às metodologias de aprendizagem.....	85
Figura 41 - Opinião dos alunos sobre o trabalho.....	85

LISTA DE TABELAS

Tabela 1 - Alfabeto deslocado 3 casas - Cifra de César.....	24
Tabela 2 - Alfabeto associado a um número (mod 27) - Adaptado da Cifra de Hill.....	60

SUMÁRIO

1	INTRODUÇÃO	15
2	REFERENCIAL TEÓRICO	19
2.1	Criptografia e sua evolução na história	19
2.1.1	Cifra de substituição e de transposição	21
2.1.2	Bastão de Licurgo ou Skytale (Cítala espartana)	23
2.1.3	Cifra de Políbio ou Quadrado de Políbio	23
2.1.4	Cifra de César	23
2.1.5	Cifra de Vigenère	25
2.1.6	Cifra de Hill	26
2.2	Criptoanálise	26
2.2.1	Análise de frequências das letras	28
2.2.2	Criptografia moderna na 1ª e 2ª Guerra Mundial	28
2.2.3	Criptografia com algoritmo de chave simétrica e de chave assimétrica	30
2.3	Criptografia e o ensino de matemática	33
3	FUNDAMENTAÇÃO MATEMÁTICA	35
3.1	Matrizes	35
3.1.1	Definição de matrizes	35
3.1.2	Adição e Subtração de matrizes	37
3.1.3	Multiplicação de um escalar por uma matriz	38
3.1.4	Multiplicação entre matrizes	39
3.1.5	Matriz transposta	42
3.1.6	Matriz identidade	43
3.1.7	Inversa de uma matriz	44
3.2	Determinantes por expansão em cofatores	46
3.3	Cofatores	47
3.4	Adjunta de uma matriz	51

3.5	A inversa de uma matriz usando sua adjunta.....	52
3.6	Aritmética modular.....	53
4	ATIVIDADES RELACIONANDO CRIPTOGRAFIA E MATRIZES.....	56
4.1	Atividade 1 - A César, o que é de César!	57
4.2	Atividade 2 - Cifra-me!	60
4.3	Atividade 3 - Decifra-me! Se for capaz!	63
4.4	Atividade 4 - Top Secret!	66
5	APRESENTAÇÃO DA PESQUISA E ANÁLISE DOS RESULTADOS.....	71
6	CONSIDERAÇÕES FINAIS.....	86
	REFERÊNCIAS.....	88
	APÊNDICE A - Folhas de atividades para sala de aula.....	91
	APÊNDICE B - Questionário da pesquisa.....	95

1 INTRODUÇÃO

A constante desmotivação com a aprendizagem da matemática por parte dos alunos, gera certa frustração no ensino da matemática por parte dos professores. Dificuldades de aprendizagem em matemática podem levar a menores rendimentos e causar preocupação para os envolvidos. Segundo Gomes e Michel (2018):

A palavra motivar significa: dar motivo, causar, expor motivo; vem da palavra motivo mais o sufixo ação, que quer dizer movimento, atuação ou manifestação de uma força, ou uma energia. A motivação influencia o comportamento em diversos contextos da vida humana e em múltiplas atividades, desde as mais básicas às mais complexas (GOMES; MICHEL, 2018, p. 2).

O ensino tradicional, baseado no ensino teórico e expositivo, já não é suficiente para as necessidades escolares, sendo necessários outros métodos de ensino para complementar e motivar a aprendizagem.

A metodologia de ensino presente nas propostas didáticas deste trabalho é baseada na história da matemática, pois a história da criptografia anda de mãos dadas com a história da matemática. O desenvolvimento da criptografia deve muito à matemática, pois ela estuda e desenvolve estratégias para tornar a criptografia mais difícil de “quebrar”. D’Ambrósio (1999) pergunta, “[...] Para quem e para que serve a história da matemática?” E ele responde,

Para quem? Para alunos, professores, pais e público em geral. Para que? Algumas das finalidades principais parecem-me: 1. para situar a Matemática como uma manifestação cultural de todos os povos em todos os tempos, como a linguagem, os costumes, os valores, as crenças e os hábitos, e como tal diversificada nas suas origens e na sua evolução; 2. para mostrar que a Matemática que se estuda nas escolas é uma das muitas formas de Matemática desenvolvidas pela humanidade; 3. para destacar que essa Matemática teve sua origem nas culturas da antiguidade mediterrânea e se desenvolveu ao longo da Idade Média e somente a partir do século XVII se organizou como um corpo de conhecimentos, com um estilo próprio; 4. para saber que desde então a Matemática foi incorporada aos sistemas escolares das nações colonizadas, se tornou indispensável em todo o mundo em consequência do desenvolvimento científico, tecnológico e econômico, e avaliar as consequências sócio-culturais dessa incorporação (D’AMBRÓSIO, 1999, p.27).

A necessidade de proteger informações ou dados importantes está presente na humanidade desde os tempos mais remotos. Foi criada pelos egípcios, romanos, hindus e também por outras civilizações, cada uma à sua maneira. Elas usavam a criptografia com a mesma motivação que temos hoje: evitar que mensagens importantes caíam em mãos erradas.

A importância histórica e científica da matemática não pode ser negligenciada nos currículos escolares, pois demonstra de forma contextualizada a forte ligação entre a história da criptografia e o desenvolvimento científico da nossa sociedade. Para captar a atenção dos alunos, é necessário sensibilizá-los para o significado e a importância da aprendizagem, considerando os conhecimentos prévios que trazem do ambiente escolar e do exterior. A utilização de uma atividade didática diferenciada, que interligue conteúdos matemáticos a situações reais do cotidiano, motiva e desperta a curiosidade do aluno, influencia diretamente o desenvolvimento de habilidades na resolução de problemas.

Em vista disso e de como a criptografia tornou-se um assunto atual e presente em nossas vidas, surgiu a ideia que norteia esta pesquisa, unir criptografia e matemática, pois certas técnicas criptográficas são baseadas em vários ramos da matemática como a Álgebra Linear, Matemática Discreta e Teoria dos Números. Aplicar temas atuais e métodos dinâmicos no processo de ensino e aprendizagem na matemática, é mencionado nos Parâmetros Curriculares Nacionais (BRASIL, 1997, p. 23) de matemática, como: “A vitalidade da matemática deve-se também ao fato de que, apesar de seu caráter abstrato, seus conceitos e resultados têm origem no mundo real e encontram muitas aplicações em outras ciências e em inúmeros aspectos práticos da vida diária”.

Criptografia são técnicas utilizadas para a troca de informações de uma maneira segura, isto é, uma forma de comunicação secreta em que somente o emissor e o receptor conseguem ter acesso às informações trocadas. Ela é utilizada desde a antiguidade para a troca de informações secretas, principalmente durante as guerras. Para Singh, citado por Bruna Bozano (2021), “[...] a história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de códigos e os decifradores, uma corrida armamentista intelectual que teve um forte impacto na história humana”. Motivo para que grandes estudiosos estivessem e estejam até hoje sempre em busca de quebrar a técnica criptográfica criada, visando desenvolver outra mais segura.

Atualmente, a criptografia é amplamente utilizada como meio de segurança no acesso a sistemas de caixas eletrônicos, sites da internet e outros meios que necessitam garantir a segurança da transmissão de dados.

Ao desenvolver este estudo, chegou-se ao seguinte problema de pesquisa: A criptografia pode despertar a curiosidade dos alunos e motivá-los a aprender?

O objetivo geral deste estudo é observar o processo de aprendizagem e analisar os resultados obtidos ao usar temas motivacionais, como a criptografia, em combinação com aplicações matemáticas. Para isso, temos os seguintes objetivos específicos: apresentar o conceito de criptografia e mostrar sua importância na evolução da história e da tecnologia; despertar a curiosidade dos alunos, motivando-os a fixarem conteúdos matemáticos, especificamente matrizes; relacionar criptografia e matemática através de problemas, em aplicações simples que envolvem cifras criptográficas.

Quanto aos seus objetivos, a metodologia dessa pesquisa é definida como um estudo de caráter exploratório, que envolve um levantamento bibliográfico sobre a criptografia, seus aspectos históricos e conceitos matemáticos que fundamentam o meio criptográfico. Entende-se que este método de pesquisa é adequado, pois visa compreender os comportamentos e pensamentos revelados pelos sujeitos da pesquisa no processo de desenvolvimento da situação proposta. Gil (2002) afirma que,

[...] pesquisas exploratórias têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses, [...] inclui (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que estimulem a compreensão (GIL, 2002, p. 41).

A abordagem qualitativa desta pesquisa visa descrever o resultado das informações obtidas por registros escritos e visuais das atividades realizadas pelos participantes e de um questionário, sem a mensuração quantitativa. Nessa abordagem, o autor analisa criticamente os dados coletados, fazendo uma análise valorativa, pois lê e interpreta as informações obtidas para chegar às suas próprias conclusões. Segundo Flick (2008),

As ideias centrais que orientam a pesquisa qualitativa, diferem daquelas da pesquisa quantitativa. Os aspectos essenciais da pesquisa qualitativa consistem na escolha adequada de métodos e teorias convenientes; no reconhecimento e na análise de diferentes perspectivas; nas reflexões dos pesquisadores a respeito de suas pesquisas como parte do processo de produção de conhecimento; e na variedade de abordagens e métodos (FLICK, 2008, p. 23).

A técnica de coleta de dados desta pesquisa foi a de observação participante, para isso, foram aplicadas propostas didáticas com atividades que usam a matemática, principalmente as operações matriciais com matrizes de segunda e terceira ordem, para cifrar e decifrar

mensagens. Posteriormente, os estudantes foram convidados a responder um questionário visando analisar os resultados e perceber os aspectos relevantes destas aplicações.

No capítulo 2 discutiremos sobre a criptografia apresentando um breve histórico e alguns conceitos presentes no meio criptográfico. A seguir, no capítulo 3, analisaremos a fundamentação matemática destacando o estudo de matrizes, uma vez que tal assunto é elemento principal deste trabalho. Nos capítulos 4 e 5 será comprovado a união da criptografia com a matemática, por meio de atividades que poderão guiar professores de matemática no estudo de matrizes usando algumas técnicas criptográficas. E por último, no capítulo 6 estão as considerações finais desta pesquisa.

2 REFERENCIAL TEÓRICO

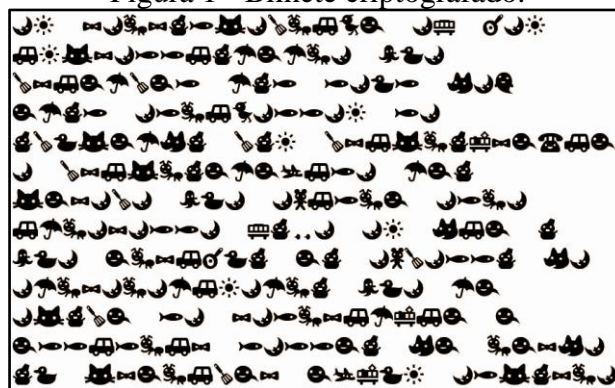
Atualmente, vivemos em tempos nos quais as informações são abundantes e a necessidade de comunicação é indispensável, mesmo sem nos darmos conta, os sistemas criptográficos estão presentes em nossas vidas, pois estão na senha do e-mail, celular ou do cartão de crédito, entre outros. Essa senha é criptografada antes de ser enviada para um servidor de internet ou para o computador central do banco para ficar protegida contra interceptação.

Neste capítulo, apresentaremos a definição de criptografia, alguns fatos históricos importantes relacionados a ela e alguns tipos de chaves criptográficas que foram e continuam sendo utilizadas na sociedade. Serão também referenciados trabalhos desenvolvidos relacionados com a criptografia e o ensino da matemática.

2.1 Criptografia e sua evolução na história

O termo criptografia surgiu da união de duas palavras gregas, “*Kryptós*” que significa escondido e “*gráphein*” que significa escrita. Em uma definição menos semântica, a criptografia são técnicas de transpor uma mensagem da sua forma original para outra ilegível, de modo que essa mensagem possa ser compreendida apenas pelo destinatário, garantindo assim o sigilo na comunicação.

Figura 1 - Bilhete criptografado.



Fonte: Página da internet Medium¹.

¹ Disponível em: <https://ricardomatsumura.medium.com/uma-introdu%C3%A7%C3%A3o-%C3%A0-criptografia-e98cfa585b26>
Acesso em: 04 nov. 2022.

O bilhete na Figura 1, é um exemplo simplório de mensagem secreta, resultado de um processo de criptografia. A criptografia é um assunto atual, mas não é um tema novo e nem simples. O manuscrito Voynich, Figura 2, por exemplo, existe há uns 600 anos e ainda não foi decifrado.

Figura 2 - Páginas do manuscrito Voynich.



Fonte: Página da internet National geographic².

A criptografia estuda métodos para codificar mensagens em que apenas o destinatário legítimo consegue interpretá-las. Segundo Fiarresga (2010), os objetivos da criptografia são:

Confidencialidade - mantém o conteúdo da informação secreto para todos excepto para as pessoas que tenham acesso à mesma; Integridade da informação - assegura não haver alteração, intencional ou não, da informação por pessoas não autorizadas; Autenticação de informação - serve para identificar pessoas ou processos com quem se estabelece comunicação; não repudição - evita que qualquer das partes envolvidas na comunicação negue o envio ou a recepção de uma informação (FIARRESGA, 2010, p. 4).

Portanto, o objetivo central da criptografia é garantir que apenas o remetente e o destinatário de uma mensagem possam ter acesso ao seu conteúdo, ou seja, a mensagem é criptografada pelo remetente e descriptografada pelo destinatário. Segundo Singh (1999),

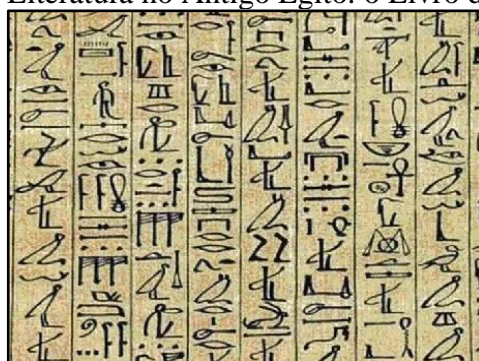
O objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado – um processo conhecido como encriptação. Para tornar a mensagem incompreensível, o texto é misturado de acordo com um protocolo específico, que já foi estabelecido previamente pelo transmissor e receptor (SINGH, 1999, p. 26).

² Disponível em: <https://nationalgeographic.pt/images/edições especiais/cultura/GrandesEnigmas/Voynich/c1.jpg>
Acesso em: 04 nov. 2022.

Uma criptografia eficiente não é decifrada rapidamente (ou quebrada, termo geralmente utilizado) por outros indivíduos diferentes do remetente e do destinatário e possibilita que o destinatário tenha acesso ao conteúdo da mensagem, revertendo a encriptação. De certa forma, a história da criptografia pode ser dividida em dois momentos, um no qual os sistemas criados eram considerados seguros, impedindo que a mensagem capturada fosse decifrada, e em outro, em que já havia muitos recursos para quebrar a mensagem criptografada. O grande desafio do primeiro momento era quebrar o código e, no segundo, inventar constantemente novos métodos para dificultar o trabalho dos decodificadores.

Primitivas técnicas de criptografia já existiam na antiguidade e a maioria das civilizações antigas parece ter usado algum nível de criptografia. As primeiras histórias sobre a utilização da criptografia, aconteceram em aproximadamente 1900 a.C., quando os egípcios utilizaram os hieróglifos (Figura 3) para codificar documentos importantes. A substituição de símbolos, uma forma mais básica de criptografia, aparece tanto nos antigos escritos egípcios, quanto nos mesopotâmicos.

Figura 3 - Literatura no Antigo Egito: o Livro dos Mortos.



Fonte: Página da internet Brasil Escola³.

Segue uma breve descrição de alguns tipos de cifras utilizadas ao longo do seu movimento histórico.

2.1.1 Cifra de substituição e de transposição

Antes de citar alguns exemplos de cifras, precisa-se saber que existem dois tipos de métodos de cifrar, o método de cifragem por substituição e método de cifragem por transposição. No primeiro método, a mensagem é codificada de modo que cada um dos seus

³ Disponível em: <https://brasilecola.uol.com.br/historiag/a-literatura-antigo-egito.htm> . Acesso em: 27 jan. 2023.

caracteres é substituído por outro de acordo com uma tabela de substituição. As cifras de substituição podem ser ainda classificadas como cifra de substituição monoalfabética, na qual as letras do texto cifrado podem ser substituídas por letras ou símbolos e cifra de substituição polialfabética, em que uma mesma letra do texto claro pode ser substituída por diferentes símbolos ou letras no texto cifrado. Segundo Ganassoli e Schankoski (2015),

A criptografia de transposição foi usada poucas vezes ao longo da história, isso se deve ao fato de que para mensagens curtas, ou para palavras de ordem de comando esse método é extremamente inseguro, visto que as letras das mensagens são reorganizadas, gerando um anagrama (GANASSOLI; SCHANKOSKI, 2015, p. 6).

O segundo método de cifragem permite que as letras permutem, ou seja, há apenas uma troca de posição entre as letras do texto não codificado e o cifrado, fazendo com que as letras permaneçam com seu significado.

2.1.2 Bastão de Licurgo ou Skytale (Cítala espartana)

A cidade-estado grega de Esparta surgiu por volta do século V a.C. A maioria de seus cidadãos eram antidemocráticos, a retórica e a cultura respeitadas pela vizinha cidade-estado de Atenas estavam longe das preocupações espartanas. Os espartanos, regidos por uma rígida cultura de guerra, preocupavam-se muito com a segurança das comunicações militares. Isso deu impulso a diferentes formas de codificar mensagens. O exemplo mais proeminente deste período é a Scytale (cítala espartana) ou Bastão de Licurgo, observável na Figura 4.

Figura 4 - Bastão de Licurgo ou Cítala espartana.



Fonte: Página da internet Png Wing⁴.

⁴ Disponível em: <https://www.pngwing.com/pt/search?q=criptografia>. Acesso em: 25 jan. 2023.

A criptografia feita com a cítila espartana consistia em enrolar um pano ou tira de couro em torno de um bastão de madeira de certa largura. A frase a ser cifrada era escrita na tira enrolada, após, era desenrolada, disfarçada como um cinto e enviada. O receptor para decifrar a mensagem recebida, enrola a tira em um bastão da mesma largura do que a mensagem foi cifrada.

2.1.3 Cifra de Políbio ou Quadrado de Políbio

Outro método conhecido é a Cifra de Políbio ou quadrado de Políbio que foi desenvolvido pelo grego Políbio por volta de 200 a.C. a 118 a.C. É uma cifra de substituição que consiste em um quadrado 5×5 e em cada espaço, uma letra, em cada linha, um número e em cada coluna, um número, como se observa na Figura 5. Ou seja, para você escrever a letra A, esta deve ser composta por dois números sendo A = 11, D = 14 e Q = 41, sempre sendo a linha pela coluna, logo a palavra DRAGÃO ficaria como 144211221134.

Figura 5 - Quadrado de Políbio.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fonte: Página da internet Acervo Lima⁵.

2.1.4 Cifra de César

Na criptografia, a cifra de César, também conhecida como cifra de troca, código de César ou troca de César, é considerada a mais simples das antigas técnicas criptográficas já conhecidas. A cifra recebe esse nome em homenagem ao imperador romano Júlio César⁶ (Figura 6), que a usou para troca de mensagens militares com seus generais durante seu governo.

⁵ Disponível em: <https://acervolima.com/cifra-quadrada-de-polibio/> . Acesso em: 10 dez. 2022.

⁶ Caio Júlio César foi um importante militar e patricio romano, governou Roma entre 49 e 44 a.C. e foi responsável por relevantes conquistas militares que legitimaram seu poder.

Nesse método, cada letra é substituída por uma letra que aparece no alfabeto três posições à frente (ou atrás), ciclicamente.

Chamamos de código de César qualquer cifra na qual cada letra da mensagem original é substituída por outra letra, deslocada em um número fixo de posições, não necessariamente três. Segundo Singh (2011),

Estes registros são encontrados nos documentos que narram a Guerra de Gália do século I a.c. neste registro, César descreve como mandou uma mensagem para Cícero, informando que substituiu as letras do alfabeto romano por letras gregas, César, às vezes, substituída cada letra da mensagem por outra que estivesse três casas à frente do mesmo alfabeto, este método de criptografia ficou conhecido como a Cifra de César (SINGH, 2011, p. 8).

Como o alfabeto português tem 26 letras, podem existir 25 códigos de César distintos. O número de espaços deslocados é a chave de criptografia e a chave original de César tem o número 3. Com alguns truques, a cifra de César permanece indecifrável por séculos e apesar de sua simplicidade, ou justamente por causa dela, foi útil por muito tempo, em uma época em que poucas pessoas podiam lê-la.

Figura 6 - Imperador romano Júlio César.



Fonte: Página da internet Pixabay⁷.

Veja exemplo da cifra de César na Tabela 1. Observe que na primeira linha estão representadas as letras em ordem alfabética. Na segunda linha, a sequência alfabética começa com a letra D, a terceira letra depois da letra A. Esta é a chave. Em seguida, acrescentam-se as outras letras, terminando a segunda linha com as letras que foram esquecidas. Assim, a letra A

⁷ Disponível em: <https://pixabay.com/pt/vectors/j%C3%BAlio-c%C3%A9sar-romano-imperador-4206555/>
Acesso em: 10 nov. 2022.

foi substituída por D, B por E, e assim por diante. Por exemplo, com este alfabeto, a palavra “CRIFTOGRAFIA” se tornaria “FULSXRJUDIL”.

Tabela 1 - Alfabeto com deslocamento de 3 casas - Cifra de César.

Original	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
Codificado	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

Fonte: Autora, 2022.

2.1.5 Cifra de Vigenère

Os franceses também tiveram papel importante no desenvolvimento da criptografia, exemplo disso é a Cifra de Vigenère, desenvolvida pelo francês Blaise de Vigenère⁸ no século XVI. É uma cifra de substituição polialfabética que consiste na utilização de mais de um alfabeto cifrante, como pode-se perceber no quadrado da Figura 7.

Figura 7 - O quadrado da Cifra de Vigenère.

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

Fonte: Página da internet Boxentriq⁹.

A cifra indecifrável ou cifra de Vigenère é uma tabela com 25 combinações diferentes do código de César. Através de uma palavra-chave codifica-se a mensagem de modo que cada letra da mensagem é codificada pelo encontro da coluna na qual está a letra da mensagem com a linha em que está a letra da chave.

⁸ Blaise de Vigenère foi um diplomata e criptógrafo francês. Aos 17 anos entrou na carreira diplomática, e aí permaneceu por 30, retirando-se em 1570.

⁹ Disponível em: <https://www.boxentriq.com/img/vigenere-table2.png> . Acesso em: 12 nov. 2022.

A cifra de Vigenère resolve o problema da fácil decodificação que existia nas cifras monoalfabéticas. Contudo, como explica Cimino (2018, p. 40), “[...] a cifra de Vigenère demorou a pegar porque usá-la exigia tempo e esforço e, em combate, a rapidez é essencial”.

As cifras monoalfabéticas ainda eram muito utilizadas, mas quando a mensagem era decifrada esperava-se que a ação militar presente nela já tivesse acontecido. Por alguns séculos foi considerada a “cifra indecifrável”, até que em 1850 o matemático inglês Charles Babbage¹⁰ “quebrou” essa cifra.

2.1.6 Cifra de Hill

A Cifra de Hill foi inventada pelo matemático norte-americano Lester S. Hill em 1929, ela é baseada na troca de letras do alfabeto por números e usa como chave matrizes quadradas invertíveis. Esta técnica será novamente abordada e demonstrada em outra seção, pois as atividades com a resolução de problemas desta pesquisa são fundamentadas na Cifra de Hill.

2.2 Criptoanálise

A criptoanálise é a arte de decifrar o texto cifrado e/ou a lógica (chave) usada para criptografá-lo. As pessoas que participam desse esforço são denominadas criptoanalistas.

Conforme Singh (2011, p. 11), “[...] a criptoanálise só pôde ser inventada depois que a civilização atingiu um nível suficientemente sofisticado de estudo, em várias disciplinas, incluindo matemática, estatística e linguística”. Algumas técnicas de criptografia permaneceram indecifráveis por muito tempo, pois naquela época, poucas pessoas sabiam ler, quanto mais calcular, o que atrasou o surgimento da criptoanálise.

A Idade Média foi um período marcado por uma relativa recessão no campo das ideias. Era muito perigosa a troca de mensagens secretas, pois eram consideradas uma prática estranha e ligada às forças do mal. Quem a usasse poderia ser acusado de bruxaria, motivo de ter sido usada nos tribunais civis e religiosos como peças de incriminação em processos de toda a natureza. Os raros sinais históricos do uso da criptografia durante este período, tem relação a

¹⁰ Charles Babbage foi um cientista, matemático, filósofo, engenheiro mecânico e inventor inglês que originou o conceito de um computador programável junto à Condessa de Lovelace, Augusta Ada King.

hábitos de monges utilizando-a em escritas, como forma de passatempo e diversão ou em sociedades religiosas.

Figura 8 - Primeira página do manuscrito de al-Kindy.



Fonte: Página da internet MVSLIM¹¹.

Os primeiros sinais de ressurgimento da criptografia ocorreram com a Idade de Ouro da civilização árabe, que iniciou por volta do ano 750 d.C., com a descoberta do "método de análise de frequência". Segundo Daniel Donda (2020),

Métodos para quebrar códigos e cifras são bem antigos. A primeira explicação gravada, conhecida da criptoanálise, foi realizada pelo árabe Abu Yusuf Yaqub ibn Ishaq al-Sabbah al-Kindy em “Um guia em decifração de mensagens criptografadas”. Al-Kindy foi um pioneiro em criptoanálise e criptografia, desenvolveu vários métodos de criptoanálise, incluindo a análise de frequências (DONDA, 2020).

Embora o termo criptoanálise seja relativamente novo (foi inventado por William Friedman¹² na década de 1920), os métodos de quebra de códigos e cifras são muito mais antigos. A primeira explicação registrada conhecida da criptoanálise foi dada em “Um guia em decifração de mensagens criptografadas” (Figura 8), do estudioso árabe al-Kindy e foi baseado em novas técnicas matemáticas desenvolvidas pelos árabes.

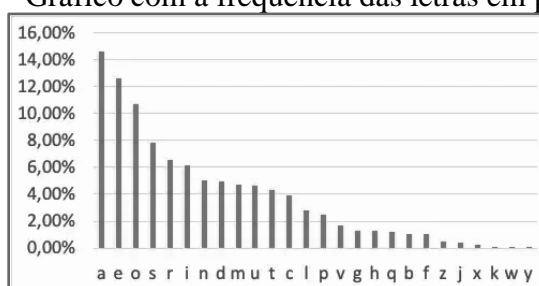
¹¹Disponível em: <https://mvslim.com/you-probably-didnt-know-al-kindis-work-on-deciphering-cryptographic-messages/> . Acesso em: 25 de jan. 2023.

¹² William F. Friedman foi um criptologista do Exército dos Estados Unidos. Ele foi o primeiro a usar o termo *criptoanálise* para se referir ao trabalho de ataque a uma cifra, em oposição à criptografia .

2.2.1 Análise de frequências das letras

A análise de frequências explora uma fraqueza fundamental nas mensagens codificadas por cifras monoalfabéticas: as diferentes frequências com que aparecem os vários símbolos.

Figura 9 - Gráfico com a frequência das letras em português.



Fonte: Página da internet Medium¹³.

A aplicação da “análise de frequências” (Figura 9) em um texto que se supõe criptografado por um código monoalfabético parte do princípio que o símbolo que aparece repetidamente na mensagem criptografada corresponderia à letra A, em seguida, o outro símbolo mais frequente seria a letra E, e assim sucessivamente. A partir deste estágio, é preciso fazer ajustes, pois algumas letras têm frequência muito próximas. Uma dose de paciência e intuição são suficientes para completar a decifragem.

O método da análise de frequências fundou a criptoanálise em bases científicas e instalou definitivamente a eterna luta entre os criadores e decifradores de códigos. A criptoanálise, também foi importantíssima para definir a nossa sociedade atual. Existem diferenças nas formas da criptografia, de acordo com Singh (2020), “[...] tecnicamente uma substituição de palavras ou frases é definida como um código e uma substituição de letras é definida como cifra”. Esta técnica provou ser muito eficiente durante a história com as cifras monoalfabéticas e polialfabéticas. Pela primeira vez, as pessoas que tentavam decifrar mensagens criptografadas tiveram acesso a um método sistemático para fazê-lo, tornando necessário que a criptografia avançasse ainda mais para continuar sendo útil.

2.2.2 Criptografia moderna na 1ª e 2ª Guerra Mundial

¹³ Disponível em: <https://ricardomatsumura.medium.com/uma-introdu%C3%A7%C3%A3o-%C3%A0-criptografia-e98cfa585b26>
Acesso em: 10 nov. 2022.

Quando foi anunciada a 1ª Guerra Mundial (1914-1918), a Grã-Bretanha rompeu os cabos de comunicação transatlânticos da Alemanha, tornando necessário que as forças alemãs usassem cabos de comunicação internacionais ou comunicações sem fio. De acordo com Ganassoli e Schankoski (2015),

Em 1894, com a descoberta do rádio, um importante meio de comunicação que serviu na época para enviar mensagens militares através do código Morse, e sem fios interligando remetente e destinatário, ficou mais fácil a interceptação das mensagens e consequentemente concedeu várias vitórias para os criptoanalistas na Primeira Guerra Mundial (GANASSOLI; SCHANKOSKI, 2015, p. 14).

Na época da 2ª Grande Guerra, a matemática da quebra de códigos foi ainda mais importante. Os aliados perceberam que a lógica matemática poderia ser usada para decifrar as mensagens alemãs, apenas se os cálculos pudessem ser feitos rapidamente. A Segunda Guerra Mundial foi o exemplo perfeito da criptografia analógica, conhecida como máquina Enigma (Figura 10), que possibilitou o envio de mensagens em códigos criptografados, sendo um dos dispositivos tecnológicos mais importantes usados na guerra. Patentada por Arthur Scherbius¹⁴, em 1918, começou a ser utilizada na Europa por volta de 1920, a codificação dessa máquina era de difícil decifração, pois era necessário ter outra máquina Enigma para poder fazer o processo de decodificação.

Figura 10 - Máquina Enigma.



Fonte: Página da internet - Revista Expansión¹⁵.

¹⁴ Arthur Scherbius foi um engenheiro elétrico alemão que inventou a máquina de cifra mecânica Enigma.

¹⁵

Disponível

em:

<https://www.expansion.com/fueradeserie/cultura/2016/12/07/58480e61e5fdea3e398b45a6.html> Acesso em: 19 jan. 2023.

A cifra da máquina Enigma foi quebrada por outra máquina, a Enigma Bomb, desenvolvida por Alan Turing¹⁶ e sua equipe. Com a Enigma quebrada, os aliados ganharam vantagem estratégica e venceram a Segunda Guerra Mundial. Neste momento da história, a criptografia é responsável pelo surgimento dos computadores.

2.2.3 Criptografia com algoritmo de chave simétrica e de chave assimétrica

Na matemática, a palavra “algoritmo” significa a sequência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas, como esquematizado na Figura 11.

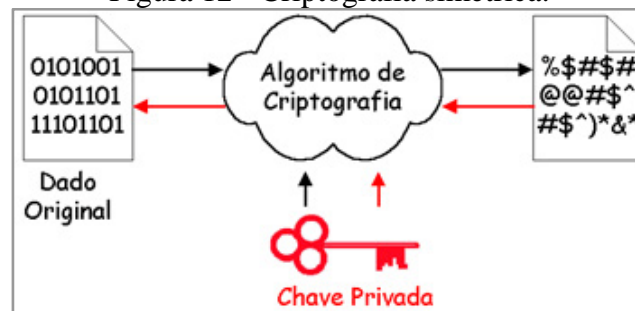
Figura 11 - Algoritmo de criptografia.



Fonte: Página da internet UFSM¹⁷.

Atualmente a segurança dos serviços de criptografia é baseado no segredo da chave que consiste em dois principais tipos: a simétrica e a assimétrica. A criptografia com algoritmo de chave simétrica é um tipo de criptografia que utiliza somente uma chave tanto para codificar como para decodificar uma mensagem, conforme Figura 12.

Figura 12 - Criptografia simétrica.



Fonte: Página da internet UFSM¹⁸.

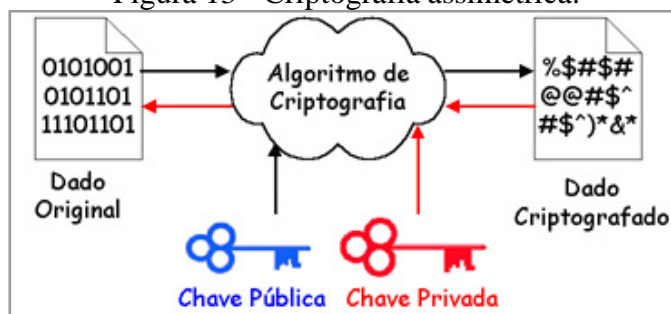
¹⁶ Alan Mathison Turing foi um matemático, cientista da computação, lógico, criptoanalista, filósofo e biólogo teórico britânico.

¹⁷ Disponível em: <https://www.ufsm.br/pet/sistemas-de-informacao/2020/05/05/introducao-a-criptografia/>
Acesso em: 22 nov. 2022.

¹⁸ Disponível em: <https://www.ufsm.br/pet/sistemas-de-informacao/2020/05/05/introducao-a-criptografia/>
Acesso em: 24 nov. 2022.

Na criptografia simétrica os algoritmos usados são mais simples que na criptografia assimétrica, levando o processo ser mais rápido, possibilitando a cifragem e a decifragem de uma grande quantidade de dados em um curto espaço de tempo curto. Segundo Fiarresga (2010, p.4), “[...] todas as criptografias eram simétricas até a década de 70, até esse momento a criptografia tinha um maior uso político e militar”.

Figura 13 - Criptografia assimétrica.



Fonte: Página da internet UFSM¹⁹.

Na criptografia com algoritmo de chave assimétrica utiliza-se duas chaves, a chave pública e a chave privada. A chave pública é usada para codificar a mensagem e a chave privada para decodificar a mensagem, como mostra o esquema da Figura 13. Os algoritmos de criptografia assimétrica só foram possíveis graças à matemática e aos recursos computacionais. A criptografia de chave assimétrica é considerada mais segura que a criptografia de chave simétrica, devido ao uso das duas chaves. Através desse método o emissor e receptor podem combinar uma chave por meio de um canal inseguro sem que um intruso possa interceptar e descobrir a chave de decodificação, esse método é baseado nas operações com logaritmos discretos. Nestes algoritmos, o emissor consegue criptografar a mensagem, mas nem ele mesmo seria capaz de decifrá-la caso não tivesse a chave-privada. Ou seja, saber codificar não implica saber decodificar. Assim, mesmo que a chave-pública, usada para criptografar a mensagem, caia em “mãos erradas”, essa pessoa não conseguiria ler a mensagem codificada. Oliveira (2012) afirma que,

Para entender o conceito, basta pensar num cadeado comum protegendo um determinado bem. A mensagem é este bem, e o cadeado, que pode ficar exposto, é a

¹⁹ Disponível em: <https://www.ufsm.br/pet/sistemas-de-informacao/2020/05/05/introducao-a-criptografia/>
Acesso em: 24 nov. 2022.

chave pública. Apenas quem tiver uma chave particular (privada) que consiga abrir o cadeado poderá acessar a mensagem (OLIVEIRA, 2012, p.2).

Em 1978 foi desenvolvida a criptografia RSA²⁰, o nome que o método recebe é em homenagem aos seus criadores, Ronald Rivest, Adi Shamir e Leonard Adleman, os quais eram professores do Instituto de Tecnologia de Massachusetts (MIT).

Pimenta (PIMENTA, 2004, p.3) diz que, “[...] os algoritmos mais utilizados na criptografia assimétrica são o RSA e o Diffie-Hellman²¹. Portanto, as mensagens criptografadas com a chave pública só podem ser descriptografadas com a chave privada correspondente do destinatário”. Baseada principalmente na teoria dos números, a criptografia RSA é considerada um dos métodos mais seguros para criptografar mensagens por ser uma criptografia de chave assimétrica e por ter como base um algoritmo que requer duas chaves, uma pública e outra privada.

A evolução dos computadores ainda continua num ritmo muito acelerado e computadores mais rápidos surgem todos os anos. Um dos grandes desafios é a fabricação do computador quântico, que, se existir, será bilhões de vezes mais rápido do que os computadores já existentes. Com isso, a criptografia poderá dar um novo grande salto. Pode-se dizer que a criptografia é considerada computacionalmente segura por dois fatores, o custo e o tempo. Quando o custo de quebrar uma criptografia excede o valor das informações criptografadas, isso significa que a criptografia foi bem-sucedida. E quando o tempo para quebrar a cifração excede a vida útil da informação, também significa que ela alcançou seu objetivo.

Além da criptografia de chave simétrica e assimétrica, existem outros tipos de chaves e ramificações das mesmas. Com o constante avanço computacional e a busca pela segurança na informação, é uma área em constante transformação. Com a promulgação da LGPD, Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), as organizações tornaram-se responsáveis pela proteção das informações que circulam internamente, bem como os dados obtidos do público. Por isso, é indispensável que as empresas e organizações em geral se preocupem em investir em mecanismos para proteger os seus usuários e dados.

²⁰ O RSA envolve um par de chaves, uma chave pública que pode ser conhecida por todos e uma chave privada que deve ser mantida em sigilo. Toda mensagem cifrada usando uma chave pública só pode ser decifrada usando a respectiva chave privada.

²¹ A troca de chaves de Diffie-Hellman é um método de criptografia para trocas de chaves de maneira segura em canais públicos. Desenvolvido por Whitfield Diffie e Martin Hellman, foi um dos primeiros exemplos práticos de métodos de troca de chaves implementado dentro do campo da criptografia, tendo sido publicado em 1976.

2.3 Criptografia e o ensino de matemática

Com relação ao levantamento bibliográfico realizado, foram selecionadas várias pesquisas com métodos de criptografia interessantes com vistas à aplicação de conceitos matemáticos. Isso nos permitiu desenvolver as atividades apresentadas neste trabalho. As referências foram coletadas em uma ferramenta de busca na internet, na qual foram encontrados inicialmente mais de 3.400 resultados, usando o filtro “criptografia e matemática”. Destes textos, selecionamos 5 (cinco) por meio dos seguintes critérios: tema central dos textos serem sobre o Ensino da Criptografia, Educação Matemática e/ou Ensino da Matemática. São eles, em ordem cronológica decrescente:

- **O uso da criptografia como ferramenta motivacional nas aulas de probabilidade no ensino médio** - por Medeiros, Macêdo e Pinheiro (2021) - Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS). Este trabalho propõe abordar em sala de aula a relação entre probabilidade e criptografia.
- **Criptografia e a Matemática** - por Oliveira (2020) - Essa pesquisa estuda o conhecimento matemático essencial para entender o sistema criptográfico mais utilizado atualmente: o sistema RSA. Entre este conhecimento matemático, os números primos se destacam na aritmética básica, e o sistema de congruência na aritmética modular. É demonstrado como funciona o sistema RSA de criptografia e como é garantida a dificuldade em quebrar a mensagem criptografada a partir dos números primos escolhidos para sua composição.
- **Explorando temas de interesse no currículo de matemática do ensino médio** - por Olgin e Groenwald (2016) - A pesquisa discute um estudo envolvendo a escolha de temas a serem trabalhados no currículo de matemática do ensino médio, que relacione os conteúdos matemáticos a temas de interesse, dentre eles a criptografia. O trabalho apresenta o uso da criptografia para ensinar função afim. Ainda classifica alguns conteúdos matemáticos possíveis de serem trabalhados usando a criptografia, dentre

eles: aritmética, aritmética modular, função linear, função quadrática, função exponencial, função logarítmica, polinômios e matrizes.

- **Criptografia e matemática** - por Ganassoli e Schankoski (2015) - Os pesquisadores sugerem várias atividades para serem aplicadas com alunos a partir do 6º ano até a 3ª série do ensino médio, que unem criptografia a diversos conteúdos de matemática, como análise combinatória, matrizes, funções, divisão, e vão além, sugerindo algumas atividades de aritmética modular e RSA.
- **Aprendendo criptologia de forma divertida** - por Bezerra, Malagutti e Rodrigues (2010) - Este trabalho faz parte de uma oficina com temas interdisciplinares da Universidade Federal da Paraíba (UFPB). O objetivo deste minicurso é apresentar atividades com criptografia envolvendo Análise Combinatória e outras curiosidades matemáticas relacionando esse tema, que podem ser aplicadas no ensino fundamental e médio.

Esses foram alguns trabalhos com publicações na área, pesquisados conforme descritos anteriormente.

3 FUNDAMENTAÇÃO MATEMÁTICA

A criptografia pode utilizar muitos conteúdos matemáticos, mas evidenciaremos apenas o estudo de matrizes. Para que as atividades propostas, envolvendo criptografia, façam sentido e possam ser resolvidas é necessário o conhecimento sobre as matrizes. Para isso, temos a intenção de apresentar os conteúdos matemáticos que foram previamente abordados com os estudantes, ou seja, a definição de matrizes, alguns tipos especiais de matrizes, as operações matriciais e a matriz inversa. Além dos conteúdos de congruência e inverso modular. Tais assuntos dão subsídio para a proposta principal deste trabalho, atividades que relacionam a criptografia e aprendizagem matemática.

3.1 Matrizes

As definições apresentadas a seguir podem ser encontradas no livro “Álgebra Linear com Aplicações” de Howard Anton e Chris Rorres - 10ª edição (ANTON, 2012). No entanto, são conteúdos que podem ser adaptados de várias obras e de diversas maneiras, considerando a característica de cada professor, a realidade da turma e o foco que se queira dar.

3.1.1 Definição de matrizes

DEFINIÇÃO 1 - Uma matriz é um agrupamento retangular de números. Dizemos que os números neste agrupamento são as entradas da matriz.

Exemplo 1 - Alguns exemplos de matrizes são:

$$\begin{bmatrix} 2 & 9 \\ 0 & -1 \\ 5 & 2 \end{bmatrix}, [5 \quad 7 \quad -3 \quad 0], \begin{bmatrix} 8 & \sqrt{2} & 1 \\ \frac{1}{4} & 0 & \pi \\ -4 & 12 & 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 5 \end{bmatrix}, [21].$$

Uma matriz com somente uma coluna é denominada matriz coluna, ou vetor coluna, e uma matriz com somente uma linha é denominada matriz linha, ou vetor linha. No exemplo 1, a matriz 2×1 é um vetor coluna, a matriz 1×4 é um vetor linha e a matriz 1×1 é um vetor coluna.

O tamanho de uma matriz é descrito em termos do número de linhas (fileiras horizontais) e de colunas (fileiras verticais) que ela contém. Por exemplo, a primeira matriz do

exemplo 1 tem três linhas e duas colunas, portanto, seu tamanho é 3 por 2 (e escrevemos 3×2). Numa descrição de tamanho, o primeiro número sempre denota o número de linhas e o segundo, o de colunas. As outras matrizes do exemplo 1 têm tamanhos 1×4 , 3×3 , 2×1 e 1×1 , respectivamente. Utilizamos letras maiúsculas para denotar matrizes e letras minúsculas para denotar quantidades numéricas, assim, podemos escrever:

$$A = \begin{bmatrix} 1 & 0 & 4 \\ 3 & 2 & -1 \\ 6 & 1 & 3 \end{bmatrix} \text{ ou } C = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

Quando discutimos matrizes, é costume dizer que as quantidades numéricas são escalares, e escalares são números reais.

A entrada que ocorre na linha i e coluna j de uma matriz A é denotada por a_{ij} . Assim, uma matriz arbitrária $m \times n$ pode ser escrita como:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}$$

e uma matriz arbitrária $m \times n$ como:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

Quando for desejada uma notação mais compacta, a matriz precedente pode ser escrita como:

$$\left[a_{ij} \right]_{m \times n} \text{ ou } \left[a_{ij} \right]$$

Sendo utilizada a primeira notação, quando for importante na argumentação, saber o tamanho da matriz, e a segunda quando o tamanho não necessitar ênfase. Em geral, combinamos a letra denotando a matriz com a letra denotando suas entradas; assim, para uma matriz B , costumamos usar b_{ij} para a entrada na linha i e na coluna j e para uma matriz C , usamos a notação c_{ij} . A entrada na linha i e na coluna j de uma matriz A também é comumente denotada pelo símbolo $(A)_{ij}$. Assim, para a matriz (1) acima, temos $(A)_{ij} = a_{ij}$ e, para a matriz:

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

temos: $(A)_{11} = 4, (A)_{12} = 0, (A)_{21} = 2$ e $(A)_{22} = -1$.

Vetores linha e coluna são de importância especial, e é prática comum denotá-los por letras minúsculas em negrito em vez de letras maiúsculas. Para tais matrizes, é desnecessário usar índices duplos para as entradas.

Assim, um vetor linha $1 \times n$ arbitrário \mathbf{a} e um vetor coluna $m \times 1$ arbitrário \mathbf{b} podem ser escritos como:

$$\mathbf{a} = [a_{11} \ a_{12} \ \dots \ a_n] \text{ e } \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

Dizemos que uma matriz A com n linhas e n colunas é uma matriz quadrada de ordem n e que as entradas destacadas $a_{11}, a_{22}, \dots, a_{m \times n}$ constituem a diagonal principal de A .

$$A = \begin{bmatrix} \mathbf{a}_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & \mathbf{a}_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & \mathbf{a}_{mn} \end{bmatrix}$$

Para algumas aplicações matemáticas é desejável desenvolver uma “aritmética de matrizes” na qual as matrizes podem ser somadas, subtraídas e multiplicadas de alguma maneira útil. O restante desta seção será dedicado a desenvolver essa aritmética.

3.1.2 Adição e Subtração de matrizes

DEFINIÇÃO 2 - Se A e B são matrizes de mesmo tamanho, então a soma $A + B$ é a matriz obtida somando as entradas de B às entradas correspondentes de A , e a diferença $A - B$ é a matriz obtida subtraindo as entradas de B das entradas correspondentes de A . Matrizes de tamanhos distintos não podem ser somadas ou subtraídas. Em notação matricial, se $A = [a_{ij}]$ e $B = [b_{ij}]$ têm o mesmo tamanho, então:

$$(A + B)_{ij} = (A)_{ij} + (B)_{ij} = a_{ij} + b_{ij} \text{ e } (A - B)_{ij} = (A)_{ij} - (B)_{ij} = a_{ij} - b_{ij}$$

Exemplo 3 - Adição e subtração - Considere as matrizes:

$$A = \begin{bmatrix} 3 & 5 & 6 & -1 \\ 2 & 1 & -3 & 0 \\ 0 & -2 & 9 & 4 \end{bmatrix}, B = \begin{bmatrix} 2 & 3 & -2 & 12 \\ 6 & -10 & 0 & 4 \\ 1 & 7 & 22 & 5 \end{bmatrix}, C = \begin{bmatrix} 7 & 4 \\ 0 & -1 \end{bmatrix}$$

Então:

$$A+B = \begin{bmatrix} 5 & 8 & 4 & 11 \\ 8 & -9 & -3 & 4 \\ 1 & 5 & 31 & 9 \end{bmatrix} \quad e \quad A-B = \begin{bmatrix} 1 & 2 & 8 & -13 \\ -4 & 11 & -3 & -4 \\ -1 & -9 & -13 & -1 \end{bmatrix}$$

As expressões $A + C$, $B + C$, $A - C$ e $B - C$ não podem ser definidas.

3.1.3 Multiplicação de um escalar por uma matriz

DEFINIÇÃO 3 - Se A for uma matriz e c um escalar, então o produto $c.A$ é a matriz obtida pela multiplicação de cada entrada da matriz A por c . Dizemos que a matriz $c.A$ é um múltiplo escalar de A . Em notação matricial, se $A = [a_{ij}]$, então: $(cA)_{ij} = c(A)_{ij} = ca_{ij}$.

Exemplo 4 - Múltiplos escalares - Para as matrizes:

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

temos:

$$2.A = \begin{bmatrix} 8 & 0 & 10 \\ 4 & -6 & -4 \\ 2 & 12 & -4 \end{bmatrix}, (-3).B = \begin{bmatrix} 0 & -21 \\ 3 & -27 \\ -6 & -6 \end{bmatrix}, \left(\frac{1}{2}\right).C = \begin{bmatrix} \frac{4}{2} & -\frac{8}{2} \\ \frac{6}{2} & \frac{10}{2} \end{bmatrix} = \begin{bmatrix} 2 & -4 \\ 3 & 5 \end{bmatrix}$$

É usual denotar $(-1).B$ por $-B$.

Até aqui, definimos a multiplicação de uma matriz por um escalar, mas não a multiplicação de duas matrizes. Como as matrizes são somadas somando as entradas correspondentes e subtraídas subtraindo as entradas correspondentes, pareceria natural definir

a multiplicação de matrizes multiplicando as entradas correspondentes. Contudo, ocorre que tal definição não seria muito útil na maioria dos problemas. A experiência levou os matemáticos à seguinte definição, muito mais útil, de multiplicação de matrizes.

3.1.4 Multiplicação entre matrizes

DEFINIÇÃO 4 - Se A for uma matriz $m \times r$ e B uma matriz $r \times n$, então o produto $A.B$ é a matriz $m \times n$ cujas entradas são determinadas como segue. Para obter a entrada na linha i e coluna j de $A.B$, destacamos a linha i de A e a coluna j de B . Multiplicamos as entradas correspondentes da linha e da coluna e então somamos os produtos resultantes.

Exemplo 5 - Multiplicando matrizes - Considere as matrizes:

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

Como A é uma matriz 3×3 e B é uma matriz 3×2 , o produto $A.B$ é uma matriz C de tamanho 3×2 .

$$A \cdot B = C$$

$$\begin{bmatrix} 4 & 0 & 5 \\ 2 & -3 & -2 \\ 1 & 6 & -2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 7 \\ -1 & 9 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \\ c_{31} & c_{32} \end{bmatrix}$$

Para determinar, por exemplo, a entrada na linha 1 e coluna 2 de $A.B$, destacamos a linha 1 de A e a coluna 2 de B . Então, como ilustrado, multiplicamos as entradas correspondentes e somamos esses produtos.

$$\begin{bmatrix} 4 & 0 & 5 \\ 2 & -3 & -2 \\ 1 & 6 & -2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 7 \\ -1 & 9 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} \square & \boxed{38} \\ \square & \square \\ \square & \square \end{bmatrix}$$

$$c_{12} = (4 \cdot 7 + 0 \cdot 9 + 5 \cdot 2) = (28 + 0 + 10) = 38$$

A entrada na linha 3 e coluna 1 de $A.B$ é calculada como segue:

$$\begin{bmatrix} 4 & 0 & 5 \\ 2 & -3 & -2 \\ 1 & 6 & -2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 7 \\ -1 & 9 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} \boxed{} & \boxed{38} \\ \boxed{} & \boxed{} \\ \boxed{-10} & \boxed{} \end{bmatrix}$$

$$c_{31} = [1 \cdot 0 + 6 \cdot (-1) + (-2) \cdot 2] = (0 - 6 - 4) = -10$$

As contas para as demais entradas são:

$$\begin{aligned} c_{11} &= 4 \cdot 0 + 0 \cdot (-1) + 5 \cdot 2 = 0 + 0 + 10 = 10 \\ c_{21} &= 2 \cdot 0 + (-3) \cdot (-1) + (-2) \cdot 2 = 0 + 3 - 4 = -1 \\ c_{22} &= 2 \cdot 7 + (-3) \cdot 9 + (-2) \cdot 2 = 14 - 27 - 4 = -17 \\ c_{32} &= 1 \cdot 7 + 6 \cdot 9 + (-2) \cdot 2 = 7 + 54 - 4 = 57 \end{aligned}$$

$$A \cdot B = \begin{bmatrix} 10 & 38 \\ -1 & -17 \\ -10 & 57 \end{bmatrix}$$

A definição de multiplicação de matrizes exige que o número de colunas do primeiro fator A seja igual ao número de linhas do segundo fator B para ser possível formar o produto A.B. Se essa condição não for satisfeita, o produto não estará definido. Uma maneira conveniente de determinar se o produto de duas matrizes está ou não definido é escrever o tamanho do primeiro fator e, à direita, escrever o tamanho do segundo fator. Se, como em (1), os números internos coincidirem, então o produto estará definido

$$\begin{array}{ccc} A & \cdot & B & = & C \\ \mathbf{m} \times \mathbf{r} & & \mathbf{r} \times \mathbf{n} & & \mathbf{m} \times \mathbf{n} \end{array} \quad (1)$$

Exemplo 6 - Determinando se um produto está definido: Suponha que A, B e C sejam matrizes de tamanhos:

$$\begin{array}{ccc} A & B & C \\ 3 \times 4 & 4 \times 7 & 7 \times 3 \end{array}$$

Então, por (1), o produto A.B está definido e é uma matriz 3×7 , B.C está definido e é uma matriz 4×3 , e C.A está definido e é uma matriz 7×4 . Os produtos A.C, C.B e B.A não estão definidos. Em geral, se $A = [a_{ij}]$ é uma matriz $m \times r$ e $B = [b_{ij}]$ é uma matriz $r \times n$, então, conforme destacado em (2):

$$A \cdot B = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & & \vdots \\ \mathbf{a_{i1}} & \mathbf{a_{i2}} & \dots & \mathbf{a_{ir}} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mr} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} & \dots & \mathbf{b_{1j}} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & \mathbf{b_{2j}} & \dots & b_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ b_{r1} & b_{r2} & \dots & \mathbf{b_{rj}} & \dots & b_{rn} \end{bmatrix} \quad (2)$$

a entrada $(AB)_{ij}$ na linha i e coluna j de $A \cdot B$ é dada por:

$$(AB)_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \dots + a_{ir}b_{rj}$$

Propriedades da multiplicação matricial: Nem todas as leis da aritmética real são válidas na aritmética matricial. Por exemplo, sabemos que na aritmética real sempre vale $a \cdot b = b \cdot a$, sendo a lei da comutatividade da multiplicação. Na aritmética matricial, contudo, a igualdade de $A \cdot B$ e $B \cdot A$ pode ser inválida por três razões possíveis:

- 1 - $A \cdot B$ pode ser definida e $B \cdot A$ não. Por exemplo, se A é uma matriz 2×3 e B é 3×4 .
- 2 - $A \cdot B$ e $B \cdot A$ podem ambas estar definidas, mas têm tamanhos diferentes. Por exemplo, se A é uma matriz 2×3 e B é 3×2 .
- 3 - $A \cdot B$ e $B \cdot A$ podem ambas estar definidas e ter o mesmo tamanho, mas as matrizes podem diferir (conforme ilustrado no exemplo seguinte).

Exemplo 7 - A ordem é importante na multiplicação matricial - Considere as matrizes:

$$A = \begin{bmatrix} 2 & 0 \\ 3 & -1 \end{bmatrix} \quad e \quad B = \begin{bmatrix} 5 & 1 \\ -2 & 4 \end{bmatrix}$$

Multiplicando, obtemos:

$$A.B = \begin{bmatrix} 2.5+0.(-2) & 2.1+0.4 \\ 3.5+(-1).(-2) & 3.1+(-1).4 \end{bmatrix} = \begin{bmatrix} 10+0 & 2+0 \\ 15+2 & 3-4 \end{bmatrix} = \begin{bmatrix} 10 & 2 \\ 17 & -1 \end{bmatrix}$$

e

$$B.A = \begin{bmatrix} 5.2+1.3 & 5.0+1.(-1) \\ (-2).2+4.3 & (-2).0+4.(-1) \end{bmatrix} = \begin{bmatrix} 10+3 & 0-1 \\ -4+12 & 0-4 \end{bmatrix} = \begin{bmatrix} 13 & -1 \\ 8 & -4 \end{bmatrix}$$

Assim, $A.B \neq B.A$.

Observação - Não veja mais do que está escrito no exemplo 7. O exemplo não proíbe a possibilidade de $A.B$ e $B.A$ serem iguais em certos casos, somente que não são iguais em todos os casos. Se acontecer de $A.B = B.A$ dizemos que as matrizes A e B comutam.

3.1.5 Matriz transposta

DEFINIÇÃO 5 - Se A for uma matriz $m \times n$ qualquer, então a transposta de A , denotada por A^T , é definida como a matriz $n \times m$ resultante da troca das linhas com as colunas de A ; ou seja, a primeira coluna de A^T é a primeira linha de A , a segunda coluna de A^T é a segunda linha de A , e assim por diante.

Exemplo 8 - Algumas transpostas - Alguns exemplos de matrizes e suas transpostas são os seguintes:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}, B = \begin{bmatrix} 3 & 5 \\ 1 & 4 \\ -2 & 7 \end{bmatrix}, C = [3 \ 5 \ 1], D = [6]$$

Observe que não só as colunas de A^T são as linhas de A , mas também as linhas de A^T , são as colunas de A . Assim, a entrada na linha i e coluna j de A^T é a entrada na linha j e coluna i de A ; ou seja:

$$(A^T)_{ij} = (A)_{ji}$$

Observe a reversão de índices. No caso especial, em que a matriz A é uma matriz quadrada, a transposta de A pode ser obtida pela troca das entradas posicionadas simetricamente

em relação à diagonal principal. Em (3), podemos ver em que A^T também pode ser obtida “refletindo” A em torno de sua diagonal principal.

$$A = \begin{bmatrix} 4 & 0 & 5 \\ 2 & -3 & -2 \\ 1 & 6 & -1 \end{bmatrix} \rightarrow \begin{bmatrix} \color{blue}{4} & \textcircled{0} & \textcircled{5} \\ \textcircled{2} & \color{blue}{-3} & \textcircled{-2} \\ \textcircled{1} & \textcircled{6} & \color{blue}{-1} \end{bmatrix} \rightarrow \begin{bmatrix} 4 & 2 & 1 \\ 0 & -3 & 6 \\ 5 & -2 & -1 \end{bmatrix}$$

↑

Permutamos entradas

posicionadas simetricamente

em relação à diagonal principal.

(3)

3.1.6 Matriz identidade

Uma matriz quadrada com entradas 1 na diagonal principal e demais entradas nulas é denominada matriz identidade. Alguns exemplos são:

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

Uma matriz identidade é denotada pela letra I . Se for importante enfatizar seu tamanho, escrevemos I_n para a matriz identidade de tamanho $n \times n$. Para explicar o papel das matrizes identidade na aritmética matricial, consideremos o efeito de multiplicar uma matriz A de tamanho 2×3 nos dois lados por uma matriz identidade.

Multiplicando à direita pela matriz identidade 3×3 , obtemos:

$$A \cdot I_3 = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} = A$$

e multiplicando pela esquerda pela matriz identidade 2×2 , obtemos:

$$I_2 \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} = A$$

O mesmo resultado vale em geral, ou seja, se A for uma matriz $m \times n$, então:

$$A \cdot I_n = A \text{ e } I_m \cdot A = A$$

3.1.7 Inversa de uma matriz

Na aritmética real, cada número não nulo a tem um recíproco a^{-1} . ($1/a$) com a propriedade: $a \cdot a^{-1} = a^{-1} \cdot a = 1$. O número a^{-1} também é denominado inverso multiplicativo de a . Nosso próximo objetivo é desenvolver para a aritmética matricial um análogo desse resultado. Com esse objetivo, apresentamos a seguinte definição:

DEFINIÇÃO 6 - Se A for uma matriz quadrada e se pudermos encontrar uma matriz B de mesmo tamanho tal que $A \cdot B = B \cdot A = I$, então diremos que A é invertível (ou não singular) e que B é uma inversa de A. Se não puder ser encontrada uma tal matriz B, diremos que A é não invertível ou singular.

Observação - A relação $A \cdot B = B \cdot A = I$ permanece inalterada pela troca de A por B, de modo que se A for invertível e B uma inversa, então também vale que B é invertível e que A é uma inversa de B. Assim, se $A \cdot B = B \cdot A = I$, dizemos que A e B são inversas uma da outra.

Exemplo 9 - Uma matriz invertível - Sejam:

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

então:

$$A \cdot B = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$B \cdot A = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Assim, A e B são invertíveis e uma é inversa da outra.

Propriedades das inversas: É razoável perguntar se uma matriz invertível pode ter mais de uma inversa. O próximo teorema mostra que a resposta é não – uma matriz invertível tem exatamente uma inversa.

TEOREMA 1 - Se B e C são ambas inversas da matriz A, então $B = C$.

Prova: Como B é uma inversa de A, temos $B \cdot A = I$. Multiplicando ambos os lados à direita por C, dá $(B \cdot A) \cdot C = I \cdot C = C$. Mas também vale que $(B \cdot A) \cdot C = B \cdot (A \cdot C) = B \cdot I = B$, de modo que $C = B$. Como consequência desse importante resultado, podemos agora falar “dá” inversa de uma matriz invertível. Se A for invertível, então sua inversa será denotada pelo símbolo A^{-1} . Assim: $A \cdot A^{-1} = I$ e $A^{-1} \cdot A = I$.

A inversa de A desempenha na aritmética matricial praticamente o mesmo papel que o recíproco A^{-1} desempenha nas relações numéricas $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Na próxima seção, desenvolvemos um método para encontrar a inversa de matrizes invertíveis de qualquer tamanho. Por enquanto, temos o teorema seguinte, que especifica condições sob as quais uma matriz 2×2 é invertível e fornece uma fórmula simples para a inversa.

TEOREMA 2 - A matriz:

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

é invertível se, e só se, $ad - bc \neq 0$, caso onde a inversa é dada pela fórmula:

$$A^{-1} = \frac{1}{\det(A)} \cdot \begin{vmatrix} d & -b \\ -c & a \end{vmatrix}$$

Confirma-se a validade da fórmula (4), mostrando que $A \cdot A^{-1} = A^{-1} \cdot A = I$

Observação - A quantidade $a.d = b.c$ no teorema 2 é denominada determinante da matriz A de tamanho 2×2 denotada por $\det(A) = a.d - b.c$ ou, alternativamente, por:

$$\det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = a.d - b.c$$

Exemplo 10 - Calculando a inversa de uma matriz 2×2 - Em cada parte, determine se a matriz é invertível. Se for, calcule sua inversa.

$$(a) A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad (b) A = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$$

Solução (a): O determinante de A é $\det(A) = (1.4) - (2.3) = 4 - 6 = -2$, não nulo. Assim, A é invertível e sua inversa é:

$$A^{-1} = -\frac{1}{2} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -\frac{4}{2} & \frac{2}{2} \\ -\frac{3}{2} & -\frac{1}{2} \end{bmatrix} \rightarrow A^{-1} = \begin{bmatrix} -2 & 1 \\ -\frac{3}{2} & -\frac{1}{2} \end{bmatrix}$$

Deixamos para o leitor confirmar que $A \cdot A^{-1} = A^{-1} \cdot A = 1$.

Solução (b): A matriz não é invertível porque $\det(A) = (1.2) - (2.1) = 0$.

3.2 Determinantes por expansão em cofatores

Nesta seção, definimos a noção de “determinante”. Isso nos dará condições para obter uma fórmula específica para a inversa de uma matriz invertível.

Lembre-se do teorema 2, que diz que a matriz 2×2

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

é invertível se $a.d - b.c \neq 0$ e que a expressão $a.d - b.c$ é denominada determinante da matriz A.

Lembre, também, que esse determinante é denotado escrevendo:

$$\det(A) = ad - bc \quad \text{ou} \quad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \quad (4)$$

e que a inversa de A pode ser expressa em termos do determinante por:

$$A^{-1} = \frac{1}{\det(A)} \cdot \begin{vmatrix} d & -b \\ -c & a \end{vmatrix} = ad - bc \quad (5)$$

ADVERTÊNCIA: É importante não esquecer que $\det(A)$ é um número, enquanto A é uma matriz.

3.3 Cofatores

Um dos principais objetivos desta seção é o de obter análogos da fórmula 5 que sejam aplicáveis a matrizes quadradas de todas as ordens. Para isso, é conveniente usar entradas com índices ao escrever matrizes ou determinantes. Assim, definimos o determinante de uma matriz $A = (a_{11})$ de tamanho 1×1 por $\det(A) = \det(a_{11}) = a_{11}$, e uma matriz 2×2 por:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

as duas equações em (4) tomam a forma:

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = (a_{11} \cdot a_{22}) - (a_{12} \cdot a_{21}) \quad (6)$$

A definição seguinte é fundamental para o nosso objetivo de definir o determinante de uma matriz de ordem superior.

DEFINIÇÃO 7 - Se A for uma matriz quadrada, então o menor da entrada a_{ij} é denotado por M_{ij} , e definido como o determinante da submatriz que sobra quando suprimimos a i -ésima linha e a j -ésima coluna de A . O número $(-1)^{i+j} \cdot M_{ij}$ denotado por C_{ij} e denominado cofator da entrada.

Exemplo 11 - Encontrando menores e cofatores - Seja:

$$A = \begin{bmatrix} -1 & 2 & 3 \\ 4 & 5 & 2 \\ -3 & 1 & 0 \end{bmatrix}$$

O menor da entrada a_{11} é:

$$M_{11} = \begin{vmatrix} -1 & 2 & 3 \\ 4 & 5 & 2 \\ -3 & 1 & 0 \end{vmatrix} = \begin{vmatrix} 5 & 2 \\ 1 & 0 \end{vmatrix} = (5 \cdot 0) - (2 \cdot 1) = 0 - 2 = -2 \rightarrow M_{11} = -2$$

O cofator de a_{11} é: $c_{11} = (-1)^{1+1} \cdot M_{11} \rightarrow M_{11} = -2$

Analogamente, o menor da entrada a_{32} é:

$$M_{32} = \begin{vmatrix} -1 & 2 & 3 \\ 4 & 5 & 2 \\ -3 & 1 & 0 \end{vmatrix} = \begin{vmatrix} -1 & 3 \\ 4 & 2 \end{vmatrix} = [(-1) \cdot 2] - (3 \cdot 4) = (-2) - 12 = -14 \rightarrow M_{32} = -14$$

O cofator de a_{32} é: $C_{32} = (-1)^{3+2} \cdot M_{32} \rightarrow -M_{32} = 14$

Observe que um menor M_{ij} e seu cofator correspondente C_{ij} são ou iguais ou negativos um do outro, e que o sinal $(-1)^{i+j}$ que os relaciona é +1 ou -1 conforme o padrão de tabuleiro de xadrez:

$$\begin{bmatrix} + & - & + & - & + & \dots \\ - & + & - & + & - & \dots \\ + & - & + & - & + & \dots \\ - & + & - & + & - & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}$$

Por exemplo: $C_{11} = M_{11}$, $C_{21} = -M_{21}$, $C_{22} = M_{22}$ e assim por diante. Assim, realmente nunca é preciso calcular $(-1)^{i+j}$ para encontrar C_{ij} basta calcular o menor M_{ij} e ajustar o sinal, se necessário, conforme o padrão do tabuleiro de xadrez.

Exemplo 12 - Expansão em cofatores de uma matriz 2×2 - O padrão de tabuleiro de xadrez de uma matriz $A = [a_{ij}]$ de tamanho 2×2 é:

$$\begin{bmatrix} + & - \\ - & + \end{bmatrix}$$

de modo que:

$$\begin{aligned} C_{11} &= M_{11} = a_{22} & C_{12} &= -M_{12} = -a_{21} \\ C_{21} &= -M_{21} = -a_{12} & C_{22} &= M_{22} = a_{11} \end{aligned}$$

Definição de um determinante geral

TEOREMA 3 - Se A for uma matriz $n \times n$, então independentemente de qual linha ou coluna escolhermos, sempre obteremos o mesmo número multiplicando as entradas daquela linha ou coluna pelos cofatores correspondentes e somando os produtos obtidos.

Esse resultado nos permite apresentar a próxima definição.

DEFINIÇÃO 8 - Se A for uma matriz de tamanho $n \times n$, então o número obtido multiplicando as entradas de uma linha ou coluna qualquer de A pelos cofatores correspondentes e somando os produtos assim obtidos é denominado determinante de A. As próprias somas são denominadas expansão em cofatores de $\det(A)$, ou seja,

$$\det(A) = a_{i1}C_{i1} + a_{i2}C_{i2} + \dots + a_{in}C_{in} \rightarrow \text{Expansão em cofatores ao longo da linha } i, \text{ e}$$

$$\det(A) = a_{1j}C_{1j} + a_{2j}C_{2j} + \dots + a_{nj}C_{nj} \rightarrow \text{Expansão em cofatores ao longo da coluna } j.$$

EXEMPLO 13 - Expansão em cofatores ao longo da primeira linha - Encontre o determinante da matriz:

$$A = \begin{bmatrix} 1 & -3 & 3 \\ 2 & 5 & -1 \\ -2 & 0 & 4 \end{bmatrix}$$

expandindo em cofatores ao longo da primeira linha.

Solução:

$$A = \begin{vmatrix} 1 & -3 & 3 \\ 2 & 5 & -1 \\ -2 & 0 & 4 \end{vmatrix} = 1 \cdot \begin{vmatrix} 5 & -1 \\ 0 & 4 \end{vmatrix} + 3 \cdot \begin{vmatrix} 2 & -1 \\ -2 & 4 \end{vmatrix} + 3 \cdot \begin{vmatrix} 2 & 5 \\ -2 & 0 \end{vmatrix} =$$

$$= 1 \cdot 20 + 3 \cdot 6 + 3 \cdot 10 = 20 + 18 + 30 = 68$$

EXEMPLO 14 - Expansão em cofatores ao longo da primeira coluna - Seja A a matriz do exemplo 3. Calcule $\det(A)$ expandindo em cofatores ao longo da primeira coluna de A.

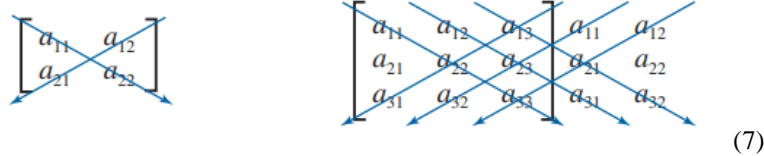
Solução:

$$A = \begin{vmatrix} 1 & -3 & 3 \\ 2 & 5 & -1 \\ -2 & 0 & 4 \end{vmatrix} = 1 \cdot \begin{vmatrix} 5 & -1 \\ 0 & 4 \end{vmatrix} - 2 \cdot \begin{vmatrix} -3 & 3 \\ 0 & 4 \end{vmatrix} - 2 \cdot \begin{vmatrix} -3 & 3 \\ 5 & -1 \end{vmatrix} =$$

$$1 \cdot 20 - 2 \cdot (-12) - 2 \cdot (-12) = 20 + 24 + 24 = 68$$

Isso confirma o resultado obtido no exemplo 13.

Uma técnica útil para calcular determinantes 2×2 e 3×3



ADVERTÊNCIA: A técnica de setas só funciona com determinantes de matrizes 2×2 e 3×3.

No caso 2×2, o determinante pode ser calculado formando o produto das entradas na seta para a direita e subtraindo o produto das entradas na seta para a esquerda.

No caso 3×3, primeiro copiamos as primeira e segunda colunas conforme indicado em (7) e depois podemos calcular o determinante somando o produto das entradas nas setas para a direita e subtraindo os produtos das entradas nas setas para a esquerda. Esse procedimento executa as seguintes contas.

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \cdot \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \cdot \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \cdot \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} =$$

$$a_{11} \cdot (a_{22} \cdot a_{33} - a_{23} \cdot a_{32}) - a_{12} \cdot (a_{21} \cdot a_{33} - a_{23} \cdot a_{31}) + a_{13} \cdot (a_{21} \cdot a_{32} - a_{22} \cdot a_{31}) =$$

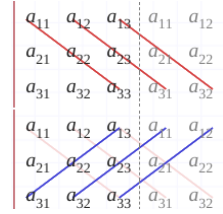
$$a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{13} \cdot a_{22} \cdot a_{31} - a_{12} \cdot a_{21} \cdot a_{33} - a_{11} \cdot a_{23} \cdot a_{32}$$

que estão de acordo com a expansão em cofatores ao longo da primeira linha.

Exemplo 15 - Regra de Sarrus - Uma técnica para calcular determinantes de matriz 2×2 e 3×3:

$$(a) \det(A) = \begin{vmatrix} 4 & 2 \\ 3 & 1 \end{vmatrix} = \begin{vmatrix} 4 & 2 \\ 3 & 1 \end{vmatrix} \times = (4 \cdot 1) - (2 \cdot 3) = 4 - 6 = -2 \rightarrow \det(A) = -2$$

$$(b) \det(A) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = +a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{13} \cdot a_{22} \cdot a_{31} - a_{11} \cdot a_{23} \cdot a_{32} - a_{12} \cdot a_{21} \cdot a_{33}$$



$$(c) \det(A) = \begin{vmatrix} 1 & 2 & -3 \\ 3 & 4 & -1 \\ 0 & -2 & 5 \end{vmatrix} \begin{vmatrix} 1 & 2 \\ 3 & 4 \\ 0 & -2 \end{vmatrix} = 1 \cdot 4 \cdot 5 + 2 \cdot (-1) \cdot 0 + (-3) \cdot 3 \cdot (-2) - 0 \cdot 4 \cdot (-3) - (-2) \cdot (-1) \cdot 1 - 5 \cdot 3 \cdot 2 \rightarrow 20 + 0 + 18 + 0 - 2 - 30 = 38 - 32 = 6 \rightarrow \det(A) = 6$$

TEOREMA 3 - Uma matriz quadrada A é invertível se, e só se, $\det(A) \neq 0$.

Exemplo 16 - Testando invertibilidade por determinantes - Como a primeira e terceira linhas de:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 0 & 1 \\ 3 & 6 & 9 \end{bmatrix}$$

são proporcionais, $\det(A) = 0$. Assim, A não é invertível. Agora estamos prontos para o principal resultado relativo a produtos de matrizes.

3.4 Adjunta de uma matriz

DEFINIÇÃO 9 - Se A for uma matriz $n \times n$ qualquer e C_{ij} o cofator de a_{ij} , então a matriz

$$\begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix}$$

é denominada matriz de cofatores de A . A transposta desta matriz é denominada adjunta de A e denotada por $\text{adj}(A)$.

Exemplo 17 - A adjunta de uma matriz 3×3 - Seja:

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & 1 \\ -1 & 2 & 1 \end{bmatrix}$$

Os cofatores de A são: $C_{11} = 1$ $C_{12} = 1$ $C_{13} = -3$
 $C_{21} = -2$ $C_{22} = 1$ $C_{23} = 0$
 $C_{31} = 2$ $C_{32} = -1$ $C_{33} = 3$

de modo que a matriz dos cofatores é:

$$C = \begin{bmatrix} 1 & -2 & 2 \\ 1 & 1 & -1 \\ -3 & 0 & 3 \end{bmatrix}$$

e a adjunta de A é:

$$\text{adj}(A) = \begin{bmatrix} 1 & 1 & -3 \\ -2 & 1 & 0 \\ 2 & -1 & 3 \end{bmatrix}$$

No teorema 2, apresentamos uma fórmula para a inversa de uma matriz 2×2 invertível. Nosso próximo teorema estende aquele resultado para matrizes invertíveis $n \times n$.

3.5 A inversa de uma matriz usando sua adjunta

TEOREMA 4 - Se A for uma matriz invertível, então:

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A)$$

Prova: Em primeiro lugar, mostramos que $A \cdot \text{adj}(A) = \det(A) \cdot I$. Considere o produto:

$$A \cdot \text{adj}(A) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ \mathbf{a_{i1}} & \mathbf{a_{i2}} & \dots & \mathbf{a_{in}} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} c_{11} & c_{12} & \dots & \mathbf{c_{j1}} & \dots & c_{n1} \\ c_{21} & c_{22} & \dots & \mathbf{c_{j2}} & \dots & c_{n2} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{1n} & c_{2n} & \dots & \mathbf{c_{jn}} & \dots & c_{nn} \end{bmatrix}$$

A entrada na i -ésima linha e j -ésima coluna do produto $A \cdot \text{adj}(A)$ é:

$$a_{i1}C_{j1} + a_{i2}C_{j2} + \dots + a_{in}C_{jn} \quad (8)$$

(ver as linhas destacadas nas matrizes). Se $i = j$, então (8) é a expansão em cofatores de $\det(A)$ ao longo da i -ésima linha de A e se $i \neq j$, então as entradas da matriz A e os cofatores provêm de linhas diferentes de A , de modo que o valor de (8) é zero. Portanto:

$$A \cdot \text{adj}(A) = \begin{bmatrix} \det(A) & 0 & \dots & 0 \\ 0 & \det(A) & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \det(A) \end{bmatrix} = \det(A) \cdot I \quad (9)$$

Como A é invertível, $\det(A) \neq 0$. Portanto, a equação (9) pode ser reescrita como:

$$\frac{1}{\det(A)} \cdot [A \cdot \text{adj}(A)] = I \quad \text{ou} \quad A \cdot \left[\frac{1}{\det(A)} \cdot \text{adj}(A) \right] = I$$

Multiplicando ambos lados à esquerda por A^{-1} , resulta:

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A)$$

Exemplo 18 - Usando a adjunta para encontrar uma matriz inversa.

Solução: Deixamos para o leitor conferir que $\det(A) = -1$. Assim:

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A) = (-1) \cdot \begin{bmatrix} 1 & 1 & -3 \\ -2 & 1 & 0 \\ 2 & -1 & 3 \end{bmatrix} = \begin{bmatrix} -1 & -1 & 3 \\ 2 & -1 & 0 \\ -2 & 1 & -3 \end{bmatrix}$$

3.6 Aritmética modular

A operação mod 26 corresponde a uma operação de aritmética modular da definição de Anton (2012, p.657). No exemplo 20, substituímos os inteiros maiores do que 25 pelo seu resto

da divisão por 26. Essa técnica de trabalhar com os restos é a base de uma parte da Matemática denominada aritmética modular.

Na aritmética modular, supomos dado um inteiro positivo m , denominado módulo, e consideramos “iguais” ou “equivalentes” em relação ao módulo quaisquer dois inteiros cuja diferença seja um múltiplo inteiro do módulo. Mais precisamente, temos a definição seguinte:

DEFINIÇÃO 10 - Dados um número inteiro positivo m e dois inteiros a e b quaisquer, dizemos que a é equivalente a b módulo m , e escrevemos: $a \cong b \pmod{m}$, se $a \cong b$ for um múltiplo inteiro de m .

Exemplo 19 - Várias equivalências:

$$\begin{array}{ll} 7 = 2 & \pmod{5} \\ -1 = 25 & \pmod{26} \end{array} \qquad \begin{array}{ll} 19 = 3 & \pmod{2} \\ 12 = 0 & \pmod{4} \end{array}$$

Dado um módulo m , arbitrário, pode ser provado que qualquer inteiro a é equivalente, módulo m , a exatamente um dos inteiros: $\{0, 1, 2, \dots, m-1\}$. Esse inteiro é denominado resíduo de a módulo m e escrevemos para denotar o conjunto dos resíduos módulo m : $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$. Se a for um inteiro não negativo, então seu resíduo módulo m é simplesmente o resto da divisão de a por m . Para um inteiro a arbitrário, o resíduo pode ser encontrado usando o seguinte teorema.

TEOREMA 5 - Dados um inteiro a e um módulo m quaisquer, seja:

$$R = \text{resto de } \frac{|a|}{m}$$

Então o resíduo r de a módulo m é dado por:

$$r = \begin{cases} R & \text{se } a \geq 0 \\ m - R & \text{se } a < 0 \text{ e } R \neq 0 \\ 0 & \text{se } a < 0 \text{ e } R = 0 \end{cases}$$

Exemplo 20 - Resíduos mod 26 - Encontre os resíduos módulo 26 de (a) 87, (b) 38 e (c) 26.

Solução (a): dividindo $|87| = 87$ por 26, temos um resto de $R = 9$, ou seja, $r = 9$.

Assim, $87 = 9 \pmod{26}$.

Solução (b): dividindo $|-38| = 38$ por 26, dá um resto de $R = 12$, ou seja, $r = 26 - 12 = 14$.

Assim, $38 = 14 \pmod{26}$.

Solução (c): dividindo $|-26| = 26$ por 26, temos um resto de $R = 0$. Assim, $-26 = 0 \pmod{26}$.

Na aritmética usual, cada número não nulo a tem um recíproco, ou inverso multiplicativo, denotado por a^{-1} , tal que: $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Aqui termina a apresentação dos conteúdos matemáticos necessários para o entendimento dos capítulos que virão.

4 ATIVIDADES RELACIONANDO CRIPTOGRAFIA E MATRIZES

A BNCC, Base Nacional Comum Curricular (BRASIL, 2018), é um documento normativo para a rede de ensino público e privado que determina os conhecimentos e as habilidades essenciais que todos os alunos têm o direito de aprender. Na prática, isso significa que, independentemente da região, raça ou classe socioeconômica, todos estudantes do Brasil devem aprender as mesmas habilidades e competências ao longo da sua vida escolar. As atividades que serão desenvolvidas neste trabalho, nesse contexto, tem as seguintes características:

Unidade Temática: Números e Álgebra.

Objetos de Conhecimento: Matrizes e Determinantes.

Competências específicas:

- C3 - Utilizar estratégias, conceitos e procedimentos matemáticos, em seus campos – Aritmética, Álgebra, Grandezas e Medidas, Geometria, Probabilidade e Estatística – para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.
- C4 - Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional, etc.), na busca de solução e comunicação de resultados de problemas.

Habilidades:

- (EM13MAT315) - Reconhecer um problema algorítmico, enunciá-lo, procurar uma solução e expressá-la por meio de um algoritmo, com o respectivo fluxograma.
- (EM13MAT405) - Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.

As atividades que serão apresentadas neste capítulo foram elaboradas para serem aplicadas em uma turma de 2º ano do ensino médio. A previsão do tempo de duração é de 10 horas de aula. Essa proposta didática envolve o conhecimento da história da criptografia e dos conteúdos matemáticos: matrizes e determinantes de segunda e terceira ordem, e aritmética modular (teorema do resto), que são a fundamentação matemática do capítulo anterior.

Esta pesquisa foi dividida em quatro atividades:

- Atividade 1 - A César, o que é de César! - Mensagem decifrada pela Cifra de César;
- Atividade 2 - Cifra-me! - Criptografia com multiplicação de matrizes;
- Atividade 3 - Decifra-me! Se for capaz! - Criptografia com matriz inversa de segunda ordem;
- Atividade 4 - Top Secret! - Criptografia com matriz inversa de terceira ordem.

A seguir, os modelos de como foram elaboradas e aplicadas essas atividades.

4.1 Atividade 1 - A César, o que é de César!

Mensagem cifrada e decifrada pela Cifra de César.

Duração: 2 períodos de 50 minutos cada.

Objetivo: apresentar o conceito de criptografia, dar exemplos da importância da criptografia desde a antiguidade até os dias atuais e estimular a curiosidade dos alunos sobre o tema apresentado.

Procedimentos:

1º momento: como introdução ao tema escolhido, pergunte aos alunos se já ouviram falar em cifras, se sabem o que significa e se conhecem exemplos de códigos secretos para troca de informações (troca de bilhetes). Como estímulo, podemos lembrá-los de livros ou filmes de ação, ou suspense, nos quais é preciso decifrar algum código, como: “O código da Vinci” (2006), a trilogia “Matrix” (1999) e “O jogo da imitação” (2014), entre outros.

2º momento: os alunos assistem a um vídeo sobre criptografia intitulado “A César, o que é de César!” Segundo a sinopse do vídeo, na ficção, Pedro, um adolescente especialista em tecnologia, fala com o imperador romano Júlio César (Figura 14) por meio de um programa de computador. Eles falam sobre criptografia e como as mensagens criptografadas foram importantes desde a Roma antiga até hoje, fornecendo exemplos de códigos e seu uso na história.

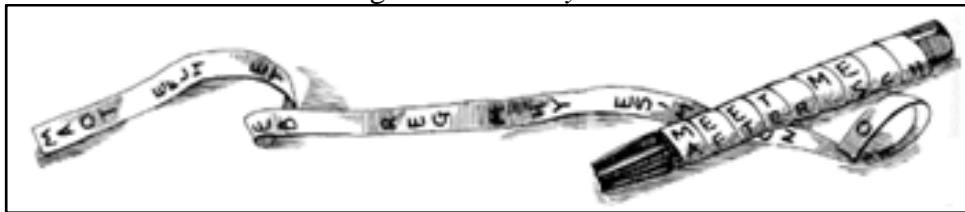
Figura 14 - Cenas do vídeo: A César, o que é de César!



Fonte: Matemática Multimídia²².

Outra técnica muito interessante de criptografia é a Skytale (Figura 15), uma técnica de criptografia muito antiga usada durante a guerra pelos espartanos. O vídeo *La Skytale*²³, mostra detalhadamente como era essa cítala.

Figura 15 - *La Skytale*.



Fonte: Página da internet UFSCAR²⁴.

3º momento: Os alunos devem formar grupos, para juntos descriptografar uma mensagem secreta criptografada usando a técnica da Cifra de César.

A atividade é realizada em folha impressa com uma mensagem criptografada anexada conforme o exemplo. A mensagem abaixo foi criptografada com a chave 3 da Cifra de César conforme Tabela 1:

Tabela 1 - Alfabeto com deslocamento de 3 casas – Cifra de César.

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

Fonte: Autora, 2022.

Mensagem codificada:

²² Disponível em: <https://youtu.be/5mPAmnqIPeS> . Acesso em: 20 nov. 2022.

²³ Disponível em: <https://youtu.be/7uq4hIV0dkU> . Acesso em: 20 nov. 2022.

²⁴ Disponível em: <https://www.dm.ufscar.br/profs/caetano/iae2004/G6/citala.htm> . Acesso em: 20 nov. 2022.

UHIOHUR - SDEOR#QHUXGD

VH#VRX#DPDGR

TXDQWR#PDLV#DPDGR

PDLV#FRUUHVSRQGR#DR#DPRU

VH#VRX#HVTXHFLGR

GHYR#HVTXHFHU#WDPHP

SRLV#R#DPRU#H#IHLWR#HVSHOKR

WHP#TXH#WHU#UHIOHUR

Mensagem decifrada conforme Tabela 1:

**U H I O H A R - S D E O R # Q H U X G D
R E F L E X O - P A B L O # N E R U D A**

**V H # V R X # D P D G R
S E # S O U # A M A D O**

**T X D Q W R # P D L V # D P D G R
Q U A N T O # M A I S # A M A D O**

**P D L V # F R U U H V S R Q G R # D R # D P R U
M A I S # C O R R E S P O N D O # A O # A M O R**

**V H # V R X # H V T X H F L G R
S E # S O U # E S Q U E C I D O**

**G H Y R # H V T X H F H U # W D P E H P
D E V O # E S Q U E C E R # T A M B É M**

**S R L V # R # D P R U # H # I H L W R # H V S H O K R
P O I S # O # A M O R # É # F E I T O # E S P E L H O**

**W H P # T X H # W H U # U H I O H A R
T E M # Q U E # T E R # R E F L E X O**

As atividades 2, 3 e 4 usam a operação mod 27, sendo uma adaptação de uma cifra de substituição conhecida como Cifra de Hill, que usa a operação mod 26, conforme atividades no trabalho de dissertação de Clarissa Melo²⁵.

4.2 Atividade 2 - Cifra-me!

Duração: 2 períodos de 50 minutos cada.

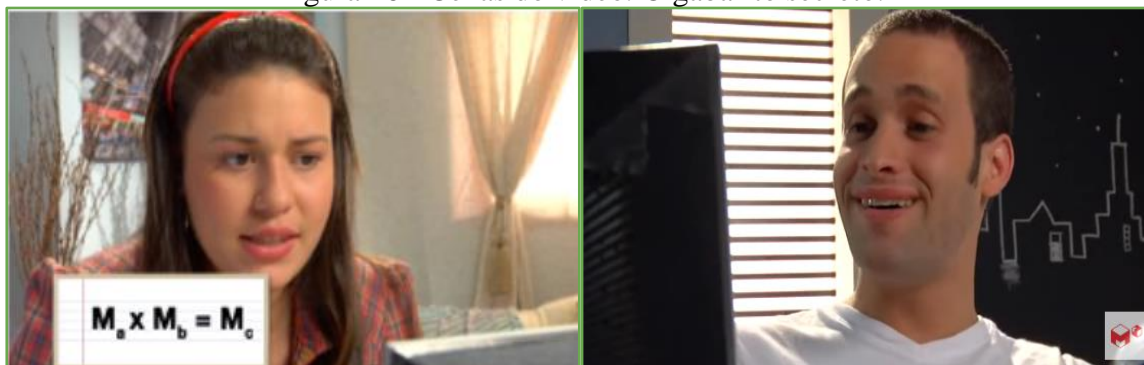
Objetivo: fixar a compreensão de multiplicação entre matrizes relacionando-a com a aplicação em criptografia.

Nesse experimento os alunos criam uma mensagem secreta e a enviam para outro grupo decifrar na atividade 3. Nesta experiência, os alunos aprenderão uma das várias maneiras de criptografar mensagens, usando matrizes inversas. O objetivo específico desta atividade é fixar conteúdos como multiplicação de matrizes conhecendo e aplicando um método diferente, ou não, daquele que o professor já apresentou em aulas anteriores. Aqui a atividade foi desenvolvida com uma matriz-chave de segunda ordem, porém, pode-se fazer o mesmo experimento com matrizes quadradas de dimensões maiores.

Procedimentos:

1º momento: para conhecer como a criptografia e a matemática se relacionam, os alunos assistem um vídeo intitulado “O gabarito secreto” (Figura 16). Conforme a sinopse do vídeo, uma jovem estudando para uma prova de matemática se depara com algumas matrizes que parecem ser uma mensagem criptografada contendo as respostas da tal prova. Com a ajuda do irmão, ela tenta decifrar a mensagem e acaba aprendendo um pouco sobre as matrizes.

Figura 16 - Cenas do vídeo: O gabarito secreto.



Fonte: Matemática Multimídia²⁶.

²⁵ Disponível em: <https://www.bdtd.uerj.br:8443/bitstream/1/17533/2/Disserta%C3%A7%C3%A3o%20-%20Clarissa%20Duarte%20Loureiro%20de%20Melo%20-%20202014%20-%20Completa.pdf.pdf> . Acesso em: 13 jan. 2023.

²⁶ Disponível em: <https://youtu.be/Jr83wILbRaM> . Acesso em: 20 nov. 2022.

2º momento: a turma é dividida em grupos de forma que o número de grupos formados seja “par”. Isso porque os grupos devem trocar mensagens criptografadas entre si ao final da atividade. A primeira tarefa da atividade é que cada grupo crie sua própria mensagem secreta usando a matriz-chave, de segunda ordem, na folha impressa, conforme orientação do professor.

Exemplo da atividade 2: para criptografar a frase “AMO MATEMÁTICA” o processo será dividido em 5 passos.

- Passo 1: A frase “AMO MATEMÁTICA”, para ser criptografada, deve se transformar em “AMO#MATEMATICA” e em seguida, a nova “palavra” é dividida em blocos de n letras. O valor de n pode variar segundo o interesse do remetente.

Para tal, usaremos a Tabela 2 para a conversão das letras para números:

Tabela 2 - Alfabeto associado a um número (mod 27).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	#	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: Autora, 2023.

- Passo 2: cada letra será associada ao número de sua posição no alfabeto.

A	M	O	#	M	A	T	E	M	A	T	I	C	A
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	12	14	26	12	0	19	4	12	0	19	8	2	0

- Passo 3: agrupar os números da mensagem original dois a dois, formando matrizes vetores 2×1 (**m**).

$$\underbrace{\begin{bmatrix} 0 \\ 12 \end{bmatrix}}_{m_1} \quad \underbrace{\begin{bmatrix} 14 \\ 26 \end{bmatrix}}_{m_2} \quad \underbrace{\begin{bmatrix} 12 \\ 0 \end{bmatrix}}_{m_3} \quad \underbrace{\begin{bmatrix} 19 \\ 4 \end{bmatrix}}_{m_4} \quad \underbrace{\begin{bmatrix} 12 \\ 0 \end{bmatrix}}_{m_5} \quad \underbrace{\begin{bmatrix} 19 \\ 8 \end{bmatrix}}_{m_6} \quad \underbrace{\begin{bmatrix} 12 \\ 0 \end{bmatrix}}_{m_7}$$

- Passo 4: para fazer o processo de codificação deve-se escolher uma matriz 2×2 que seja invertível. Pegamos como exemplo a matriz A abaixo.

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$$

Como, $\det(A) = (a_{11} \cdot a_{22}) - (a_{12} \cdot a_{21}) = (1 \cdot 3) - (2 \cdot 2) = 3 - 4 = -1 \neq 0$.

Logo, a matriz A possui inversa e é uma possível chave.

Observação: Se a matriz escolhida não for inversível, pode ocorrer de a mensagem não ser decifrável, pois sem a condição de ser inversível não podemos garantir que pontos que representam letras distintas possam ser levados a letras distintas. Na realidade, trata-se de um contexto amplo: dentre todas as infinitas matrizes 2×2 , apenas um número finito delas tornarão a mensagem impossível de ser revertida.

- Passo 5: escolhida a matriz-chave A, multiplicar a mesma por cada vetor matriz 2×1 da mensagem original (**m**).

$$\begin{aligned} A \cdot m_1 &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 12 \end{bmatrix} = \begin{bmatrix} 1 \cdot 0 + 2 \cdot 12 \\ 2 \cdot 0 + 3 \cdot 12 \end{bmatrix} = \begin{bmatrix} 0 + 24 \\ 0 + 36 \end{bmatrix} = \begin{bmatrix} 24 \\ 36 \end{bmatrix} \rightarrow (\text{mod}27) \rightarrow \begin{bmatrix} 24 \\ 9 \end{bmatrix} \rightarrow \begin{bmatrix} Y \\ J \end{bmatrix} \\ A \cdot m_2 &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 26 \end{bmatrix} = \begin{bmatrix} 1 \cdot 14 + 2 \cdot 26 \\ 2 \cdot 14 + 3 \cdot 26 \end{bmatrix} = \begin{bmatrix} 14 + 52 \\ 28 + 78 \end{bmatrix} = \begin{bmatrix} 66 \\ 106 \end{bmatrix} \rightarrow (\text{mod}27) \rightarrow \begin{bmatrix} 12 \\ 25 \end{bmatrix} \rightarrow \begin{bmatrix} M \\ Z \end{bmatrix} \\ A \cdot m_3 &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 12 + 2 \cdot 0 \\ 2 \cdot 12 + 3 \cdot 0 \end{bmatrix} = \begin{bmatrix} 12 + 0 \\ 24 + 0 \end{bmatrix} = \begin{bmatrix} 12 \\ 24 \end{bmatrix} \rightarrow (\text{mod}27) \rightarrow \begin{bmatrix} 12 \\ 24 \end{bmatrix} \rightarrow \begin{bmatrix} M \\ Y \end{bmatrix} \\ A \cdot m_4 &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \cdot 19 + 2 \cdot 4 \\ 2 \cdot 19 + 3 \cdot 4 \end{bmatrix} = \begin{bmatrix} 19 + 8 \\ 38 + 12 \end{bmatrix} = \begin{bmatrix} 27 \\ 50 \end{bmatrix} \rightarrow (\text{mod}27) \rightarrow \begin{bmatrix} 0 \\ 23 \end{bmatrix} \rightarrow \begin{bmatrix} A \\ X \end{bmatrix} \\ A \cdot m_5 &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 12 + 2 \cdot 0 \\ 2 \cdot 12 + 3 \cdot 0 \end{bmatrix} = \begin{bmatrix} 12 + 0 \\ 24 + 0 \end{bmatrix} = \begin{bmatrix} 12 \\ 24 \end{bmatrix} \rightarrow (\text{mod}27) \rightarrow \begin{bmatrix} 12 \\ 24 \end{bmatrix} \rightarrow \begin{bmatrix} M \\ Y \end{bmatrix} \\ A \cdot m_6 &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 8 \end{bmatrix} = \begin{bmatrix} 1 \cdot 19 + 2 \cdot 8 \\ 2 \cdot 19 + 3 \cdot 8 \end{bmatrix} = \begin{bmatrix} 19 + 16 \\ 38 + 24 \end{bmatrix} = \begin{bmatrix} 35 \\ 62 \end{bmatrix} \rightarrow (\text{mod}27) \rightarrow \begin{bmatrix} 8 \\ 8 \end{bmatrix} \rightarrow \begin{bmatrix} I \\ I \end{bmatrix} \\ A \cdot m_7 &= \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 2 + 2 \cdot 0 \\ 2 \cdot 2 + 3 \cdot 0 \end{bmatrix} = \begin{bmatrix} 2 + 0 \\ 4 + 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \end{bmatrix} \rightarrow (\text{mod}27) \rightarrow \begin{bmatrix} 2 \\ 4 \end{bmatrix} \rightarrow \begin{bmatrix} C \\ E \end{bmatrix} \end{aligned}$$

Fonte: Autora, 2023.

Note que na segunda multiplicação, temos um problema, pois o número 66 não possui equivalente alfabético na Tabela 2. Para resolver esse problema, realizamos o seguinte acordo:

sempre que ocorrer um inteiro maior do que 26, ele será substituído pelo resto da divisão desse inteiro por 27.

Observação: Como o resto da divisão por 27 é um dos inteiros 0, 1, 2, ..., 26, esse procedimento sempre fornece um inteiro com equivalente alfabético. Assim, substituímos 66 por 12, pois 12 é o resto da divisão de 66 por 27.

Segue da Tabela 2, que o texto cifrado do par AM é YJ e assim sucessivamente. Os demais vetores correspondem aos pares de texto cifrado MZ, MY, AX, MY, II e CE, respectivamente. Coletando os pares, obtemos a mensagem cifrada completa: YJ MZ MY AX MY II CE, que normalmente, seria transmitida como uma única cadeia sem espaços: YJMZMYAXMYIICE.

Esta mensagem cifrada será entregue, com a matriz-chave A, para outro grupo decifrar na próxima atividade.

4.3 Atividade 3 - Decifra-me! Se for capaz!

Duração: 3 períodos de 50 minutos cada.

Objetivo: aplicar o método da adjunta para calcular a inversa de uma matriz de segunda ordem para resolver o problema da mensagem criptografada.

Procedimentos:

1º momento: divide-se a turma em grupos, de modo que a quantidade de grupos formados seja um número “par”, pois esta atividade é continuação da anterior, na qual os grupos trocam entre si as mensagens. O desafio agora é decifrar a mensagem secreta recebida, usando a chave informada. A chave será uma matriz de segunda ordem que deverá ser transformada em matriz inversa, usando o método da adjunta, para desvendar o segredo da mensagem.

O professor deve explicar com exemplos no quadro como calcular a matriz inversa pelo método da adjunta e, se necessário, fazer uma questão como exercícios antes de iniciar a atividade de criptografia. Ao desenvolver a atividade, você pode fazer a seguinte pergunta aos alunos:

- Qual deve ser o tamanho da matriz vetor para que a inversa da matriz chave possa ser multiplicada pela matriz vetor da mensagem criptografada, $A^{-1} \cdot mc$? Por quê?

Exemplo da atividade 3: Esse tipo de criptografia usa chaves simétricas, ou seja, a chave para cifrar e decifrar é a mesma. Um destinatário que conhece a chave de criptografia usada

pelo remetente sabe que pode usar operações matriciais para determinar a chave de descryptografia e obter acesso à mensagem enviada. Para isso você precisa seguir estes passos:

- Passo 1: primeiro, precisamos calcular o determinante da matriz-chave A para conferir se ela é invertível. Sendo:

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}$$

Deste modo, dado que $\det(A) = -1$, esta matriz possui inversa e é uma chave.

- Passo 2: calcular a matriz inversa de A para retornar a mensagem original. O método para calcular a matriz inversa pode ser qualquer um válido, aqui é usado o método da adjunta, que também pode ser utilizado para matrizes de ordem superior a 2. Para calcular a matriz adjunta, devemos primeiro calcular a matriz C dos cofatores de A:

$$C = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

$$\begin{aligned} c_{11} &= (-1)^{1+1} \cdot |M_{11}| \Rightarrow c_{11} = (-1)^2 \cdot |3| \Rightarrow c_{11} = 1 \cdot 3 \Rightarrow c_{11} = 3 \\ c_{12} &= (-1)^{1+2} \cdot |M_{12}| \Rightarrow c_{12} = (-1)^3 \cdot |2| \Rightarrow c_{12} = (-1) \cdot 2 \Rightarrow c_{12} = -2 \\ c_{21} &= (-1)^{2+1} \cdot |M_{21}| \Rightarrow c_{21} = (-1)^3 \cdot |2| \Rightarrow c_{21} = (-1) \cdot 2 \Rightarrow c_{21} = -2 \\ c_{22} &= (-1)^{2+2} \cdot |M_{22}| \Rightarrow c_{22} = (-1)^4 \cdot |1| \Rightarrow c_{22} = 1 \cdot 1 \Rightarrow c_{22} = 1 \end{aligned}$$

A matriz C dos cofatores de A é:

$$C = \begin{bmatrix} 3 & -2 \\ -2 & 1 \end{bmatrix}$$

- Passo 3: transformar a matriz C dos cofatores de A em matriz adjunta $\underline{\underline{C}}$, dado que $\underline{\underline{C}} = C^T$.

$$\underline{\underline{C}} = \begin{bmatrix} 3 & -2 \\ -2 & 1 \end{bmatrix}$$

- Passo 4: calcular a inversa da matriz chave usando a matriz dos cofatores de A:

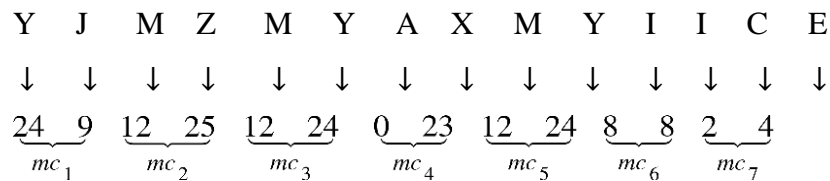
$$\begin{aligned} A^{-1} &= \frac{1}{\det(A)} \cdot \underline{\underline{C}} \rightarrow A^{-1} = \frac{1}{(-1)} \cdot \begin{bmatrix} 3 & -2 \\ -2 & 1 \end{bmatrix} \\ \rightarrow A^{-1} &= (-1) \cdot \begin{bmatrix} 3 & -2 \\ -2 & 1 \end{bmatrix} \rightarrow A^{-1} = \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix} \end{aligned}$$

- Passo 5: trocar as letras da mensagem criptografada pelos respectivos números conforme a Tabela 2 e formar os vetores da mensagem codificada (**mc**):

Tabela 2 - Alfabeto associado a um número (mod 27).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	#	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: Autora, 2023.



Observação: A matriz vetor da mensagem codificada deve ser do tamanho 2×1 para ser possível a multiplicação: $A^{-1}.mc$:

$$\begin{bmatrix} 24 \\ 9 \end{bmatrix} \begin{bmatrix} 12 \\ 25 \end{bmatrix} \begin{bmatrix} 12 \\ 24 \end{bmatrix} \begin{bmatrix} 0 \\ 23 \end{bmatrix} \begin{bmatrix} 12 \\ 24 \end{bmatrix} \begin{bmatrix} 8 \\ 8 \end{bmatrix} \begin{bmatrix} 2 \\ 4 \end{bmatrix}$$

mc_1 mc_2 mc_3 mc_4 mc_5 mc_6 mc_7

- Passo 6: multiplicamos a matriz inversa de A por cada vetor da mensagem codificada (**mc**), $A^{-1}.mc$ e encontramos:

$$A^{-1}.mc_1 = \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 24 \\ 9 \end{bmatrix} = \begin{bmatrix} -3.24+2.9 \\ 2.24-1.9 \end{bmatrix} = \begin{bmatrix} -72+18 \\ 48-9 \end{bmatrix} = \begin{bmatrix} -54 \\ 39 \end{bmatrix} \xrightarrow{(mod27)} \begin{bmatrix} 0 \\ 12 \end{bmatrix} \rightarrow \begin{bmatrix} A \\ M \end{bmatrix}$$

$$A^{-1}.mc_2 = \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 25 \end{bmatrix} = \begin{bmatrix} -3.12+2.25 \\ 2.12-1.25 \end{bmatrix} = \begin{bmatrix} -36+50 \\ 24-25 \end{bmatrix} = \begin{bmatrix} 14 \\ -1 \end{bmatrix} \xrightarrow{(mod27)} \begin{bmatrix} 0 \\ 12 \end{bmatrix} \rightarrow \begin{bmatrix} O \\ \# \end{bmatrix}$$

$$A^{-1}.mc_3 = \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 24 \end{bmatrix} = \begin{bmatrix} -3.12+2.24 \\ 2.12-1.24 \end{bmatrix} = \begin{bmatrix} -36+48 \\ 24-24 \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \end{bmatrix} \xrightarrow{(mod27)} \begin{bmatrix} 12 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} M \\ A \end{bmatrix}$$

$$\begin{aligned}
A^{-1}.mc_4 &= \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 23 \end{bmatrix} = \begin{bmatrix} -3.0 + 2.23 \\ 2.0 - 1.23 \end{bmatrix} = \begin{bmatrix} 0 + 46 \\ 0 - 23 \end{bmatrix} = \begin{bmatrix} 46 \\ -23 \end{bmatrix} \xrightarrow{(mod27)} \begin{bmatrix} 19 \\ 4 \end{bmatrix} \rightarrow \begin{bmatrix} T \\ E \end{bmatrix} \\
A^{-1}.mc_5 &= \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 24 \end{bmatrix} = \begin{bmatrix} -3.12 + 2.24 \\ 2.12 - 1.24 \end{bmatrix} = \begin{bmatrix} -36 + 48 \\ 24 - 24 \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \end{bmatrix} \xrightarrow{(mod27)} \begin{bmatrix} 12 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} M \\ A \end{bmatrix} \\
A^{-1}.mc_6 &= \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 8 \end{bmatrix} = \begin{bmatrix} -3.8 + 2.8 \\ 2.8 - 1.8 \end{bmatrix} = \begin{bmatrix} -24 + 16 \\ 16 - 8 \end{bmatrix} = \begin{bmatrix} -8 \\ 8 \end{bmatrix} \xrightarrow{(mod27)} \begin{bmatrix} 19 \\ 8 \end{bmatrix} \rightarrow \begin{bmatrix} T \\ I \end{bmatrix} \\
A^{-1}.mc_7 &= \begin{bmatrix} -3 & 2 \\ 2 & -1 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 4 \end{bmatrix} = \begin{bmatrix} -3.2 + 2.4 \\ 2.2 - 1.4 \end{bmatrix} = \begin{bmatrix} -6 + 8 \\ 4 - 4 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix} \xrightarrow{(mod27)} \begin{bmatrix} 2 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} C \\ A \end{bmatrix}
\end{aligned}$$

Fonte: Autora, 2023.

Note que na primeira multiplicação, temos um problema, pois o resultado é um número negativo -54 e não possui equivalente alfabético, pois é menor que zero (Tabela 2).

Para resolver esse problema, fazemos conforme segue do teorema 5 da Aritmética modular: dividindo $|-54| = 54$ por 27, dá um resto de $R = 2$, ou seja, $r = 27 - 2 = 25$. Assim, $-54 = 25 \pmod{27}$. Segue da Tabela 2, que o texto cifrado do par IJ é AM e assim sucessivamente. Os demais vetores correspondem aos pares de texto cifrado O#, MA, TE, MA, TI e CA respectivamente. Coletando os pares, obtemos a mensagem cifrada completa:

AM O# MA TE MÁ TI CA, que normalmente, seria transmitida como uma única cadeia sem espaços: AMO#MATEMÁTICA. Esta é a mensagem decifrada.

4.4 Atividade 4 - Top Secret!

Neste experimento, os alunos usam uma matriz maior, de terceira ordem, como chave para descriptografar uma mensagem criptografada pelo professor.

Duração: 3 períodos de 50 minutos cada.

Objetivo: incentivar o estudante a progredir no conhecimento anterior, ou seja, aplicar o método da adjunta para calcular a inversa de uma matriz de terceira ordem.

Observação: Nesta atividade, o determinante da matriz-chave escolhida pelo professor (que pode ser igual ou diferente entre os grupos) é igual a 1, para que os alunos possam facilmente calcular a matriz inversa. Pode ser feita com qualquer matriz de terceira ordem com determinante diferente de zero.

Procedimentos:

A turma é dividida em grupos, depois o professor distribui as folhas impressas das atividades. O quarto desafio é descriptografar a mensagem secreta recebida usando a chave fornecida. A chave será a matriz que precisa ser invertida para revelar o segredo da mensagem. O professor explica que a resolução pelo método da adjunta também pode ser utilizada para matrizes de tamanhos maiores que 2×2 , pois a matriz-chave nesta atividade é de terceira ordem. Por ser um pouco mais elaborada, na parte dos cofatores de A, o professor deve explicar com exemplos no quadro e, se necessário, fazer uma questão como exercício antes de iniciar a atividade de criptografia. Ao desenvolver a atividade, você pode fazer as seguintes perguntas aos alunos:

- O tamanho da matriz vetor será o mesmo da atividade anterior? Por quê?
- Qual deve ser o tamanho da matriz vetor para que a inversa da matriz chave possa ser multiplicada pela matriz vetor da mensagem criptografada, $A^{-1} \cdot mc$?

Após, os alunos devem fazer a resolução conforme o exemplo da atividade 4 a seguir:

Matriz-chave A

$$\begin{bmatrix} 1 & 1 & 1 \\ 3 & 2 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Tabela 2 - Alfabeto associado a um número (mod 27).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	#	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: Autora, 2023.

Decifre a mensagem criptografada abaixo, usando a matriz-chave A e a Tabela 2 para conversão de letras:

U X J F U G F M N K W L!

Observação: A inversa da matriz-chave é usada para retornar a mensagem original e o método da adjunta será usado para calcular essa inversa conforme segue no exemplo.

Resolução: Matriz inversa pelo método da adjunta (ou método dos cofatores).

1. Calcule a inversa da matriz que descriptografa a mensagem secreta. Isso requer calcular o determinante da matriz-chave para ver se ela é invertível. Sendo:

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 3 & 2 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Provando que $\det(A) = 1 \rightarrow \det(A) \neq 0$, então a matriz A é invertível.

2. Calcule a matriz C dos cofatores da matriz chave A:

$$C = \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix}$$

$$c_{11} = (-1)^{1+1} \cdot |M_{11}| = (-1)^2 \cdot \begin{vmatrix} 2 & 0 \\ 1 & 0 \end{vmatrix} = 1 \cdot (2 \cdot 0 - 0 \cdot 1) = 1 \cdot (0 - 0) = 1 \cdot 0 = 0$$

$$c_{12} = (-1)^{1+2} \cdot |M_{12}| = (-1)^3 \cdot \begin{vmatrix} 3 & 0 \\ 1 & 0 \end{vmatrix} = (-1) \cdot (3 \cdot 0 - 0 \cdot 1) = (-1) \cdot (0 - 0) = (-1) \cdot 0 = 0$$

$$c_{13} = (-1)^{1+3} \cdot |M_{13}| = (-1)^4 \cdot \begin{vmatrix} 3 & 2 \\ 1 & 1 \end{vmatrix} = 1 \cdot (3 \cdot 1 - 2 \cdot 1) = 1 \cdot (3 - 2) = 1 \cdot 1 = 1$$

$$c_{21} = (-1)^{2+1} \cdot |M_{21}| = (-1)^3 \cdot \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} = (-1) \cdot (1 \cdot 0 - 1 \cdot 1) = (-1) \cdot (0 - 1) = (-1) \cdot (-1) = 1$$

$$c_{22} = (-1)^{2+2} \cdot |M_{22}| = (-1)^4 \cdot \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} = 1 \cdot (1 \cdot 0 - 1 \cdot 1) = 1 \cdot (0 - 1) = 1 \cdot (-1) = -1$$

$$c_{23} = (-1)^{2+3} \cdot |M_{23}| = (-1)^5 \cdot \begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} = (-1) \cdot (1 \cdot 1 - 1 \cdot 1) = (-1) \cdot (1 - 1) = (-1) \cdot 0 = 0$$

$$c_{31} = (-1)^{3+1} \cdot |M_{31}| = (-1)^4 \cdot \begin{vmatrix} 1 & 1 \\ 2 & 0 \end{vmatrix} = 1 \cdot (1 \cdot 0 - 1 \cdot 2) = 1 \cdot (0 - 2) = 1 \cdot (-2) = -2$$

$$c_{32} = (-1)^{3+2} \cdot |M_{32}| = (-1)^5 \cdot \begin{vmatrix} 1 & 1 \\ 3 & 0 \end{vmatrix} = (-1) \cdot (1 \cdot 0 - 1 \cdot 3) = (-1) \cdot (0 - 3) = (-1) \cdot (-3) = 3$$

$$c_{33} = (-1)^{3+3} \cdot |M_{33}| = (-1)^6 \cdot \begin{vmatrix} 1 & 1 \\ 3 & 2 \end{vmatrix} = 1 \cdot (1 \cdot 2 - 1 \cdot 3) = 1 \cdot (2 - 3) = 1 \cdot (-1) = -1$$

Assim a matriz C dos cofatores de A é:

$$C = \begin{bmatrix} 0 & 0 & 1 \\ 1 & -1 & 0 \\ -2 & 3 & -1 \end{bmatrix}$$

3. Transforme a matriz C dos cofatores de A em matriz adjunta \underline{C} dado que $\underline{C} = C^T$.

$$\overline{C} = \begin{bmatrix} 0 & 1 & -2 \\ 0 & -1 & 3 \\ 1 & 0 & -1 \end{bmatrix}$$

4. Calcule a inversa da matriz chave A: a cada caractere (letra) da mensagem recebida é atribuído um número de posição no alfabeto que compõem o vetor da mensagem codificada (**mc**) conforme Tabela 2.

U	X	J	F	U	G	F	M	N	K	W	L
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
<u>20</u>	<u>23</u>	<u>9</u>	<u>5</u>	<u>20</u>	<u>6</u>	<u>5</u>	<u>12</u>	<u>13</u>	<u>10</u>	<u>22</u>	<u>11</u>
mc_1			mc_2			mc_3			mc_4		

Observação: A matriz vetor da mensagem criptografada deve ser 3×1 para existir a multiplicação, $A^{-1} \cdot mc$:

$$\begin{bmatrix} 20 \\ 23 \\ 9 \end{bmatrix} \begin{bmatrix} 5 \\ 20 \\ 6 \end{bmatrix} \begin{bmatrix} 5 \\ 12 \\ 13 \end{bmatrix} \begin{bmatrix} 10 \\ 22 \\ 11 \end{bmatrix}$$

$mc_1 \quad mc_2 \quad mc_3 \quad mc_4$

5. Em seguida, multiplique cada vetor de mensagem codificada (**mc**) pela inversa de A para encontrar a mensagem original.

$$A^{-1} \cdot mc_1 = \begin{bmatrix} 0 & 1 & -2 \\ 0 & -1 & 3 \\ 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 23 \\ 9 \end{bmatrix} = \begin{bmatrix} 0.20 + 1.23 - 2.9 \\ 0.20 - 1.23 + 3.9 \\ 1.20 + 0.23 - 1.9 \end{bmatrix} = \begin{bmatrix} 0 + 23 - 18 \\ 0 - 23 + 27 \\ 20 + 0 - 9 \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \\ 11 \end{bmatrix} \xrightarrow{(mod 27)} \begin{bmatrix} F \\ E \\ L \end{bmatrix}$$

$$A^{-1} \cdot mc_2 = \begin{bmatrix} 0 & 1 & -2 \\ 0 & -1 & 3 \\ 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 20 \\ 6 \end{bmatrix} = \begin{bmatrix} 0.5 + 1.20 - 2.6 \\ 0.5 - 1.20 + 3.6 \\ 1.5 + 0.20 - 1.6 \end{bmatrix} = \begin{bmatrix} 0 + 20 - 12 \\ 0 - 20 + 18 \\ 5 + 0 - 6 \end{bmatrix} = \begin{bmatrix} 8 \\ -2 \\ -1 \end{bmatrix} \xrightarrow{(mod 27)} \begin{bmatrix} I \\ Z \\ \# \end{bmatrix}$$

$$A^{-1} \cdot mc_3 = \begin{bmatrix} 0 & 1 & -2 \\ 0 & -1 & 3 \\ 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 12 \\ 13 \end{bmatrix} = \begin{bmatrix} 0.5 + 1.12 - 2.13 \\ 0.5 - 1.12 + 3.13 \\ 1.5 + 0.12 - 1.13 \end{bmatrix} = \begin{bmatrix} 0 + 12 - 26 \\ 0 - 12 + 39 \\ 5 + 0 - 13 \end{bmatrix} = \begin{bmatrix} -14 \\ 27 \\ -8 \end{bmatrix} \xrightarrow{(mod 27)} \begin{bmatrix} N \\ A \\ T \end{bmatrix}$$

$$A^{-1} \cdot mc_4 = \begin{bmatrix} 0 & 1 & -2 \\ 0 & -1 & 3 \\ 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 22 \\ 11 \end{bmatrix} = \begin{bmatrix} 0.10 + 1.22 - 2.11 \\ 0.10 - 1.22 + 3.11 \\ 1.10 + 0.22 - 1.11 \end{bmatrix} = \begin{bmatrix} 0 + 22 - 22 \\ 0 - 22 + 33 \\ 10 + 0 - 11 \end{bmatrix} = \begin{bmatrix} 0 \\ 11 \\ -1 \end{bmatrix} \xrightarrow{(mod 27)} \begin{bmatrix} A \\ L \\ \# \end{bmatrix}$$

Fonte: Autora, 2022.

Observe que algumas multiplicações resultam em números negativos que não têm correspondência alfabética, pois são menores que 0 (Tabela 2). Para resolver este problema, procederemos como na atividade anterior. Segue da Tabela 2, que o texto cifrado do trio UZJ é FEL e assim sucessivamente. Os demais vetores correspondem aos trios do texto cifrado FUG, FMN e KWL, respectivamente. Coletando os trios, obtemos a mensagem cifrada completa: FEL IZ# NAT AL# , que, normalmente, seria transmitida como uma única cadeia sem espaços: FELIZ NATAL! Assim termina a apresentação das 4 atividades programadas para esta proposta didática.

No próximo capítulo, faz-se a análise das aplicações destas aulas.

5 APRESENTAÇÃO DA PESQUISA E ANÁLISE DOS RESULTADOS

As dificuldades observadas no ensino da matemática e a indiferença dos alunos em relação à aprendizagem são motivos de grande preocupação. Uma forma de amenizar essas adversidades é por meio do uso de atividades didáticas que auxiliem os professores a relacionar os conteúdos de matemática com situações atuais e do mundo real, que estimulem a curiosidade e motivem os alunos a aprender.

Como é um assunto atual, a criptografia é um tema fascinante para atividades educacionais. Grande parte do desenvolvimento da criptografia foi devido à matemática, que cria estratégias para tornar a criptografia mais complexa e difícil de interpretar para aqueles que desejam usar indevidamente informações sigilosas de outras pessoas (*hackers*).

Diante disso, chegou-se ao seguinte problema: A criptografia pode despertar a curiosidade dos alunos e motivá-los a aprender?

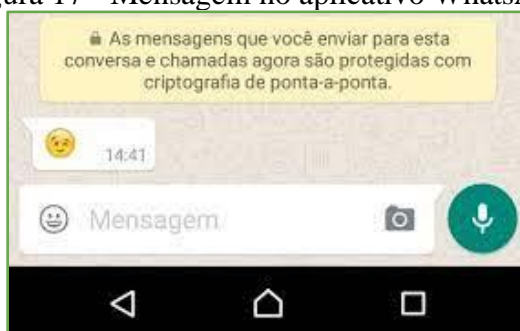
Para responder a essa pergunta, uma pesquisa foi projetada e aplicada com 16 estudantes do 2º ano do ensino médio de uma escola estadual da cidade de Esteio, no estado do Rio Grande do Sul, com idades entre 15 e 18 anos.

A análise dos dados apresentados a seguir será em ordem cronológica dos acontecimentos, considerando as 4 atividades propostas no capítulo anterior e as respostas de um questionário realizado através de uma plataforma digital online, Google Forms, organizado em dez questões. As folhas das atividades realizadas em sala de aula podem ser consultadas na íntegra nos Apêndices.

A turma teve sua primeira aula no dia 11 de novembro de 2022 e necessitou de duas aulas de 50 minutos cada para a realização da atividade 1. Este estudo foi realizado em uma sala de aula com televisão e acesso à internet.

O objetivo específico desta atividade foi estimular a curiosidade dos alunos, introduzindo o conceito de criptografia e fornecendo exemplos da importância da criptografia desde os tempos antigos até o presente. Como introdução ao tema escolhido para o desenvolvimento deste trabalho, foi perguntado se já tinham ouvido falar em criptografia e se sabiam o que significava. Eles falaram sobre o aplicativo WhatsApp, devido ao aviso que ele mostra, o de que é protegido por criptografia de ponta a ponta, como se observa na Figura 17.

Figura 17 - Mensagem no aplicativo WhatsApp.



Fonte: Página da internet Memória Ebc²⁷.

No gráfico da Figura 18, podemos observar que mais da metade, 68,8%, já sabia o que significa criptografia.

Figura 18 - Gráfico 1: quanto ao tema da pesquisa.



Fonte: Autora. Dados da pesquisa.

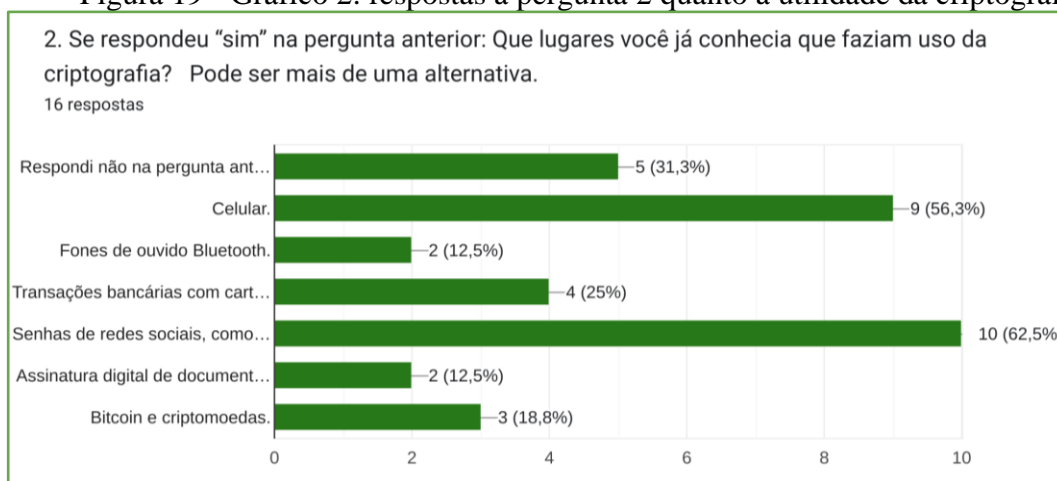
Durante a aula, para despertar ainda mais a curiosidade sobre o assunto, foi falado sobre filmes de ação ou suspense, nos quais é preciso decifrar algum código, como: “O código da Vinci” (2006), a trilogia “Matrix” (1999) e “O jogo da imitação” (2014), entre outros.

Perguntado onde mais existe criptografia, responderam que na senha do celular, das redes sociais e do cartão de crédito e, também, mencionaram os hackers que se infiltraram em redes governamentais e corporativas.

O gráfico 2, da Figura 19, mostra que as senhas de redes sociais são as mais populares entre os alunos, pois 62,5%, 10 dos 16 estudantes apontaram essa alternativa. A criptografia do fone de ouvido Bluetooth e as assinaturas digitais são as menos conhecidas em 12,5% (2 de 16).

²⁷ Disponível em: <https://images.app.goo.gl/WcfscLY92hU8Fzof8> . Acesso em: 10 nov. 2022.

Figura 19 - Gráfico 2: respostas à pergunta 2 quanto à utilidade da criptografia.



Fonte: Autora. Dados da pesquisa.

Observação: As opções que contemplam cada questão não aparecem totalmente em alguns gráficos, portanto, abaixo da figura do gráfico estão as questões correspondentes e as suas opções para melhor entendimento.

Figura 20 - Pergunta 2 e suas alternativas.

2. Se respondeu "sim" na pergunta anterior: Que lugares você já conhecia que faziam uso da criptografia?

Pode ser mais de uma alternativa.

Respondi não na pergunta anterior.

Celular.

Fones de ouvido Bluetooth.

Transações bancárias com cartão de crédito.

Senhas de redes sociais, como WhatsApp, Facebook, Instagram entre outros.

Assinatura digital de documentos.

Bitcoin e criptomoedas.

Outro: _____

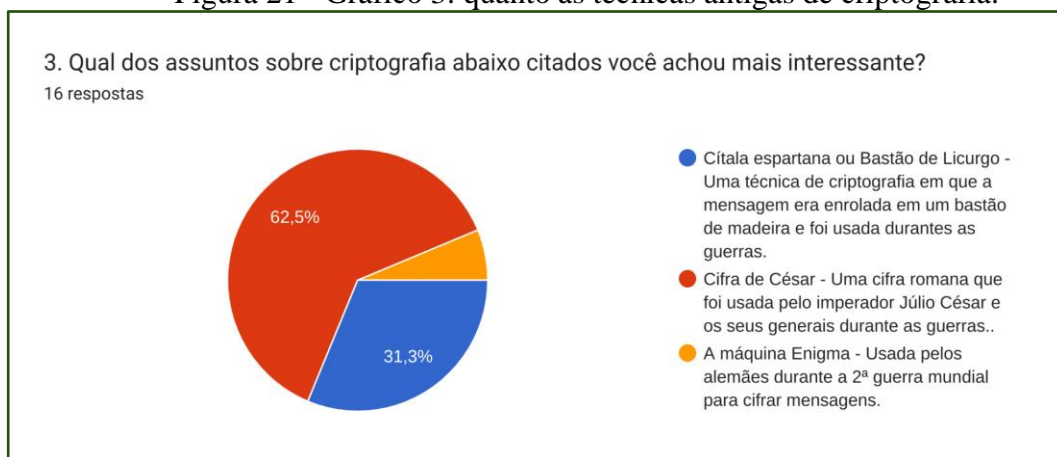
Fonte: Autora. Dados da pesquisa.

No momento seguinte, um vídeo do aplicativo YouTube sobre criptografia foi exibido na televisão, com o título: A César, o que é de César! Este episódio fala sobre cifras e a importância da cifra de César na história da humanidade.

Duas técnicas criptográficas são apresentadas no vídeo A César, o que é de César!, a cifra de César e a da máquina Enigma. Para complementar e causar curiosidade, a pesquisadora achou interessante mostrar um pequeno vídeo chamado La Skytale; a cítala; uma técnica de criptografia muito antiga usada pelos espartanos durante a guerra. Pelo que se percebe no

gráfico 3, da Figura 21, a cifra de César foi a técnica que mais chamou atenção, 62,5% dos alunos indicaram ela como a mais interessante, talvez seja pelo fato de ser a cifra trabalhada por mais tempo naquela aula.

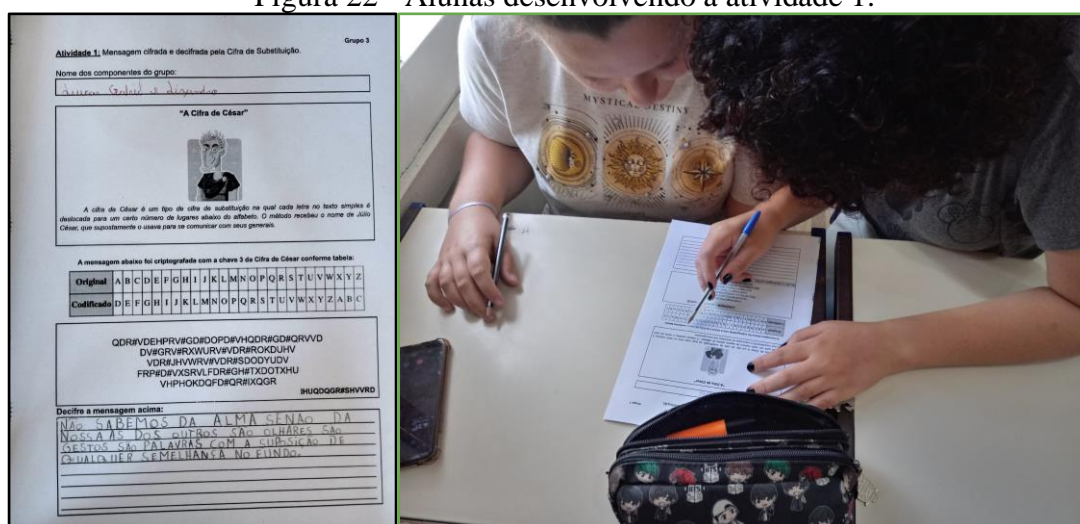
Figura 21 - Gráfico 3: quanto às técnicas antigas de criptografia.



Fonte: Autora. Dados da pesquisa.

Seguindo o planejado, a folha da atividade 1 foi entregue com uma mensagem criptografada usando a cifra de César para ser decifrada. Na Figura 22, observa-se um dos grupos respondendo à atividade 1. As mensagens revelavam uma poesia oculta e diferentes entre os grupos. Após a conclusão da tarefa, um representante de cada grupo leu a mensagem.

Figura 22 - Alunas desenvolvendo a atividade 1.



Fonte: Autora. Dados da pesquisa.

Durante a tarefa, um dos alunos perguntou se a mensagem poderia ser criptografada com um deslocamento de casas diferente, já que a chave de criptografia usada na atividade era de 3 casas. A professora respondeu que sim, porém foi esclarecido que as letras do novo texto cifrado seriam diferentes das que foram obtidas no texto com o deslocamento de 3 casas. Mas,

pelo que se percebe no gráfico 4, da Figura 23, alguns alunos (31,2%) prestaram pouca atenção ao que estava sendo dito naquele momento e responderam incorretamente à questão 4 do questionário.

Figura 23 - Gráfico 4: quanto à atividade 1 - A César, o que é de César!



Fonte: Autora. Dados da pesquisa.

A segunda aula com o grupo ocorreu no dia 18 de novembro de 2022 e exigiu duas aulas de 50 minutos cada para a realização da atividade. Isso também foi feito em sala de aula.

O objetivo específico desta atividade foi aprofundar e fixar conteúdos como multiplicação entre matrizes de uma forma divertida e interessante.

Figura 24 - [Atividade 2 resolvida por um dos grupos](#)

FOLHA 1 - Grupo 7

ATIVIDADE 2: Criptografia com matriz inversa de ordem 2.

Nome dos componentes do grupo que criou a mensagem criptografada:
Pavello e Boredo

Crie uma mensagem com no mínimo 10 letras e codifique-a usando a matriz chave abaixo e tabela para conversão conforme as instruções necessárias:

$$\begin{bmatrix} 2 & 3 \\ 9 & 14 \end{bmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z		
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Mensagem original (mínimo de 10 letras):
MADURIDADE

Codificação da mensagem (com os cálculos):

$$C.M = \begin{bmatrix} 2 & 3 \\ 9 & 14 \end{bmatrix} \cdot \begin{bmatrix} 12 & 15 & 17 & 3 & 3 \\ 0 & 20 & 8 & 0 & 4 \\ 12 & 19 & 17 & 3 & 3 \\ 0 & 20 & 8 & 0 & 4 \end{bmatrix}$$

Mensagem criptografada (apenas em letras):
YARTCGWBSC

Escreva na folha 2 a mensagem criptografada e envie para outro grupo decifrar.

Cálculos manuais na lousa:

$$\begin{pmatrix} 2 & 3 \\ 9 & 14 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 24 \\ 108 \end{pmatrix} = \begin{pmatrix} 24 \\ 108 \end{pmatrix} \rightarrow \text{A}$$

$$\begin{pmatrix} 2 & 3 \\ 9 & 14 \end{pmatrix} \cdot \begin{pmatrix} 19 \\ 20 \end{pmatrix} = \begin{pmatrix} 38 + 60 \\ 171 + 280 \end{pmatrix} = \begin{pmatrix} 98 \\ 451 \end{pmatrix} \rightarrow \text{R}$$

$$\begin{pmatrix} 2 & 3 \\ 9 & 14 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 8 \end{pmatrix} = \begin{pmatrix} 34 + 24 \\ 153 + 112 \end{pmatrix} = \begin{pmatrix} 58 \\ 265 \end{pmatrix} \rightarrow \text{T}$$

$$\begin{pmatrix} 2 & 3 \\ 9 & 14 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 \\ 27 \end{pmatrix} \rightarrow \text{E}$$

$$\begin{pmatrix} 2 & 3 \\ 9 & 14 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 6 + 12 \\ 27 + 56 \end{pmatrix} = \begin{pmatrix} 18 \\ 83 \end{pmatrix} \rightarrow \text{W}$$

$$\begin{pmatrix} 2 & 3 \\ 9 & 14 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 + 12 \\ 36 + 56 \end{pmatrix} = \begin{pmatrix} 12 \\ 92 \end{pmatrix} \rightarrow \text{B}$$

$$\begin{pmatrix} 2 & 3 \\ 9 & 14 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 20 \end{pmatrix} = \begin{pmatrix} 24 + 60 \\ 108 + 280 \end{pmatrix} = \begin{pmatrix} 84 \\ 388 \end{pmatrix} \rightarrow \text{C}$$

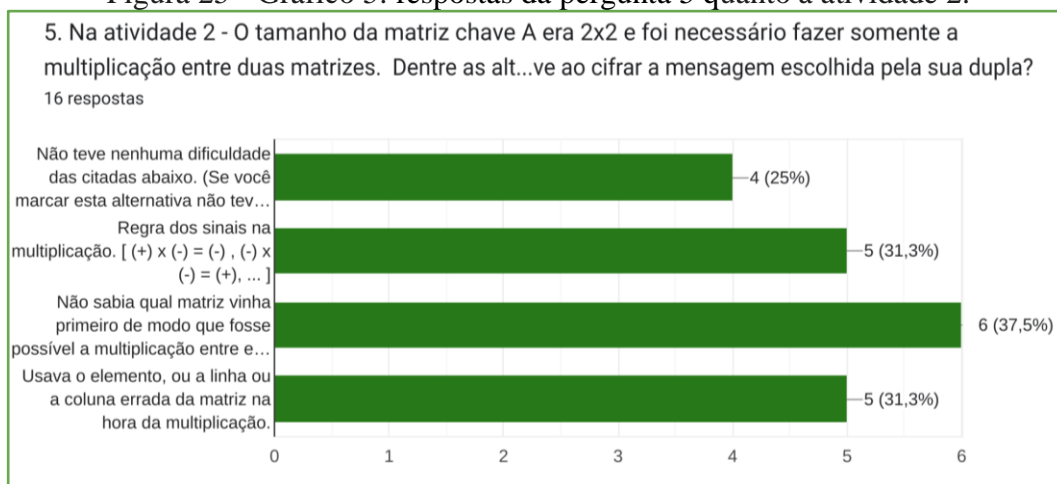
Fonte: Autora. Dados da pesquisa.

Logo no primeiro momento, foi exibido na TV um vídeo do aplicativo YouTube, com o título O gabarito secreto, que mostrava como a matemática e a criptografia estão relacionadas. Em seguida, a turma foi dividida em duplas para que o número de grupos fosse “par”, pois os grupos deveriam trocar mensagens.

Cada grupo recebeu uma folha impressa com as atividades 2 e 3. Na tarefa 2 (Figura 24), cada grupo deveria criar sua própria mensagem secreta usando a matriz de ordem 2 como chave, seguindo as instruções demonstradas no quadro.

Daremos uma olhada no gráfico 5, da Figura 25, para analisar melhor os resultados da atividade 2. Ele representa a pergunta 5 da pesquisa, na qual foi questionado qual parte da solução dificultava resolver a decodificação da mensagem escolhida pelo outro grupo.

Figura 25 - Gráfico 5: respostas da pergunta 5 quanto à atividade 2.



Fonte: Dados da pesquisa.

Figura 26 - Pergunta 5 e suas alternativas.

5. Na atividade 2 - O tamanho da matriz chave A era 2x2 e foi necessário fazer somente a multiplicação entre duas matrizes.
Dentre as alternativas citadas abaixo, quais foram as dificuldades que você teve ao cifrar a mensagem escolhida pela sua dupla?
Pode ser mais de uma alternativa.

Não teve nenhuma dificuldade das citadas abaixo. (Se você marcar esta alternativa não teve marcar as outras)

Regra dos sinais na multiplicação. [(+) x (-) = (-) , (-) x (+) = (-) , ...]

Não sabia qual matriz vinha primeiro de modo que fosse possível a multiplicação entre elas.

Usava o elemento, ou a linha ou a coluna errada da matriz na hora da multiplicação.

Outro: _____

Fonte: Autora. Dados da pesquisa.

Apenas 4 estudantes afirmaram que não tiveram dificuldade em cifrar a mensagem. Seis estudantes, ou 37,5%, disseram ter problemas com a ordem de multiplicação entre matrizes. Essa questão foi levantada e esclarecida durante a aula por um lembrete sobre as condições para as quais existe a multiplicação entre matrizes. Isso causa confusão nos alunos porque uma das maiores diferenças entre a multiplicação de números reais e a multiplicação entre matrizes, é

que a multiplicação entre matrizes não é comutativa. Em outras palavras, na multiplicação de matrizes, a ordem das matrizes multiplicadas importa. Para criptografar uma mensagem usando matrizes, precisamos multiplicar a matriz-chave 2×2 por cada uma das matrizes vetores 2×1 da mensagem original, respectivamente.

Outras dificuldades também foram apontadas na realização dessa atividade. Alguns erros foram causados pelo uso errado (troca) de elementos da linha ou coluna ao multiplicar matrizes, ou por erros nas regras de sinais. Os alunos deveriam tentar descobrir que parte da sua resolução estava errada, porque identificar os erros faz parte do processo de aprendizado, como dizem “Errando também se aprende!”, se não conseguissem, então recebiam auxílio da professora.

Concluída a tarefa, eles escreveram a mensagem criptografada em uma folha impressa, na qual já estava escrita a matriz-chave, que foi entregue a outro grupo, para que na próxima aula fosse decifrada, na atividade 3. Foi enfatizado para os alunos a importância de que a mensagem criptografada estivesse correta ao ser enviada para outro grupo decifrar, caso contrário, causaria problemas para o grupo que iria decifrá-la.

A terceira aula aconteceu no dia 22 de novembro de 2022 e exigiu 3 períodos de 50 minutos para a conclusão das atividades realizadas em sala de aula. A tarefa foi decifrar uma mensagem secreta enviada por outro grupo, da aula anterior. Com essa atividade pretende-se apresentar e ensinar um novo método de calcular a inversa de matrizes de ordem 2, relacionando matrizes e criptografia.

A chave enviada com a mensagem cifrada era uma matriz de ordem 2 e sua inversa seria necessária para desvendar o mistério da mensagem. O método para calcular matriz inversa que a turma conhecia era por sistemas lineares. Visando ensinar um novo método de resolução, foi apresentado e explicado como calcular a matriz inversa pelo método da adjunta.

Os números obtidos nas multiplicações entre a matriz inversa da chave e a matriz vetor da mensagem codificada ($A^{-1} \cdot mc$) geram o número da respectiva letra da mensagem original, exemplo: $A = 0$, $B = 1$, $C = 2$, e assim sucessivamente até chegar a $Z = 26$ e $\# = 27$ (para espaço) conforme a Tabela 2 na folha da atividade que eles possuíam.

Caso o número encontrado seja maior que 27 é preciso fazer a divisão desse número por 27, o resto dessa divisão será o número da letra correspondente e caso a divisão for exatamente o resto é 0. Para encontrar este resto foi demonstrado aos alunos como encontrá-lo na calculadora conforme o exemplo e na seguinte sequência: $106 \div 27 = 3,92592592593 - 3 =$

$0,925925925926 \times 27 = 25$. Assim, o número 25 é o resto da divisão de 106 para 27 e corresponde a letra Z na Tabela 2.

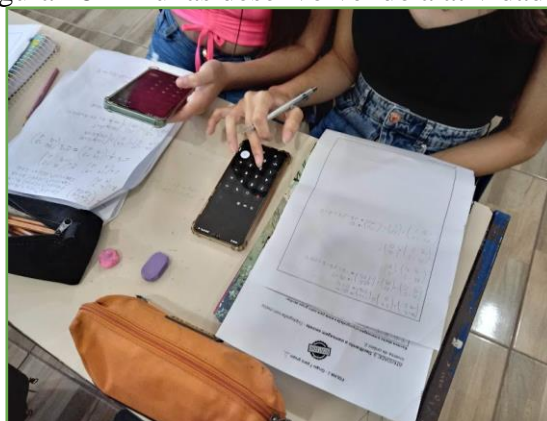
Figura 27 - Alunas comparando a atividade 3.



Fonte: Autora. Dados da pesquisa.

Após a elaboração dos cálculos alguns perceberam que algo estava errado, algumas das letras formavam uma mensagem que não tinha sentido algum. Esses erros ocorreram porque usaram os elementos, linhas ou colunas erradas ao multiplicar matrizes, também a erros na regra dos sinais na multiplicação, adição e subtração. Incertos de seu erro, eles foram ao grupo que enviou a mensagem (Figura 27), e perguntaram qual era a mensagem original e compararam com suas descobertas para ver em que parte da resolução estava o erro. Nesse momento a professora não interveio, se mesmo depois disso, não solucionasse o problema, então recebiam auxílio da professora.

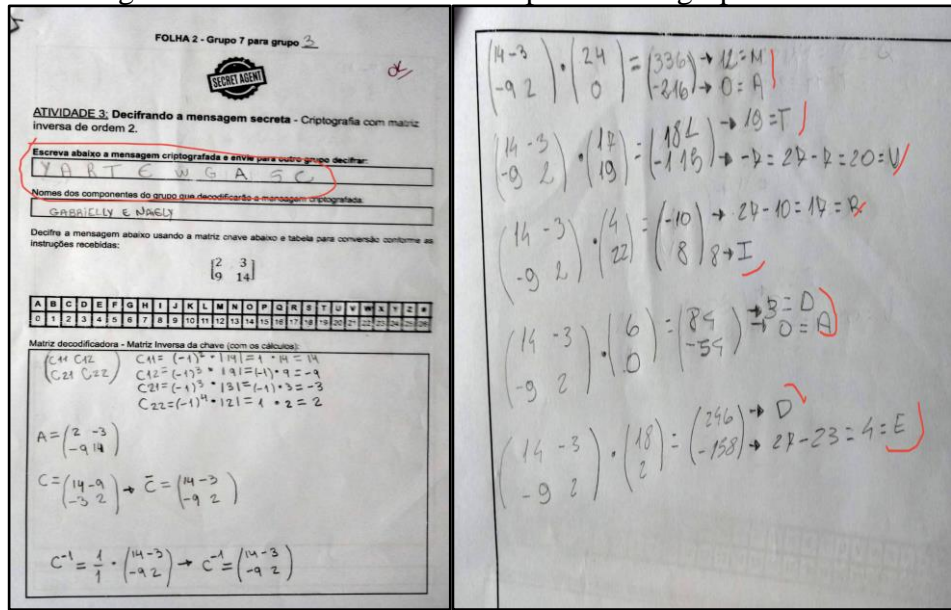
Figura 28 - Alunas desenvolvendo a atividade 3.



Fonte: Autora. Dados da pesquisa.

Devido a alguns obstáculos, a atividade não foi concluída naquele dia e teve que terminar no dia 25 de novembro de 2022. Felizmente, eles ainda estavam interessados em descobrir a mensagem criptografada e conseguiram concluir a atividade, como pode-se observar nas Figuras 28 e 29, com mais acertos no final do que erros durante o processo.

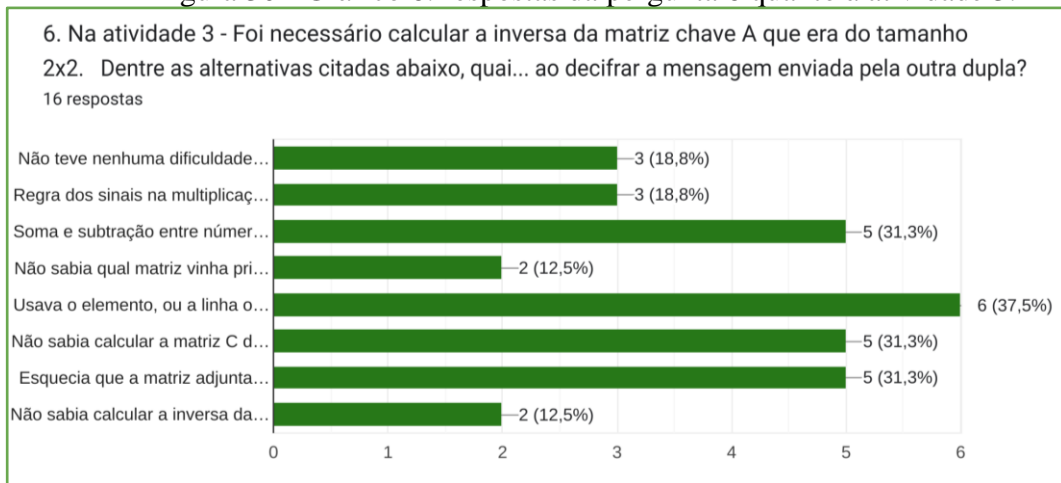
Figura 29 - Atividade 3 resolvida por um dos grupos.



Fonte: Autora. Dados da pesquisa.

Um dos objetivos deste estudo foi identificar a dificuldade dos alunos nas operações matemáticas comparando e analisando os resultados entre cada atividade.

Figura 30 - Gráfico 6: respostas da pergunta 6 quanto à atividade 3.



Fonte: Dados da pesquisa.

Figura 31 - Pergunta 6 e suas alternativas.

6. Na atividade 3 - Foi necessário calcular a inversa da matriz chave A que era do tamanho 2×2 .

Dentre as alternativas citadas abaixo, quais foram as dificuldades que você teve ao **decifrar** a mensagem enviada pela outra dupla?

Pode ser mais de uma alternativa.

Não teve nenhuma dificuldade das citadas abaixo. (Se você marcar esta alternativa não teve marcar as outras)

Regra dos sinais na multiplicação. [$(+) \times (-) = (-)$, $(-) \times (-) = (+)$, ...]

Soma e subtração entre números negativos e positivos.

Não sabia qual matriz vinha primeiro de modo que fosse possível a multiplicação entre elas.

Usava o elemento, ou a linha ou a coluna errada da matriz na hora da multiplicação

Não sabia calcular a matriz C dos cofatores de A. (Matriz do tamanho 2×2)

Esquecia que a matriz adjunta era uma matriz C transposta. (Matriz do tamanho 2×2)

Não sabia calcular a inversa da matriz chave A. (Matriz do tamanho 2×2)

Outro: _____

Fonte: Autora. Dados da pesquisa.


Segundo os resultados da atividade 3 no gráfico 6, da Figura 30, 18,8%, ou seja, 3 dos 16 alunos, indicaram que não tiveram dificuldades em resolver o problema de decifrar a mensagem, ou seja, calcular e operar com matriz inversa., o que demonstra que estavam progredindo. Apesar de ainda indicarem que tiveram alguns problemas na resolução.

A quarta aula e última atividade desta pesquisa foi realizada em 25 de novembro de 2022. Foram necessárias duas aulas de 50 minutos cada para completar a atividade. O objetivo específico desta atividade foi avançar o conhecimento do conteúdo da inversão de matrizes, agora para terceira ordem. Primeiro, foi entregue uma folha com uma mensagem criptografada, a tarefa da atividade 4 foi descriptografar a mensagem secreta usando uma chave específica. A chave era uma matriz maior, de ordem 3. Ela também precisou ser transformada em uma matriz inversa para descobrir o conteúdo da mensagem. O cálculo de matriz inversa de ordem 3, pelo método da matriz adjunta, foi explicado com exemplo no quadro e exercício.

A atividade 4, na Figura 32, mostra o erro do aluno ao calcular a matriz C dos cofatores de A, na qual alguns elementos da matriz inversa estão errados, como mostra a Figura 33, o que leva aos erros seguintes, pois mesmo que o cálculo para decifrar esteja correto, durante a multiplicação entre a inversa da matriz-chave pelo vetor da mensagem criptografada, por alguns elementos estarem errados, a mensagem descriptografada não tem o significado correto.

Figura 32 - Atividade 4 resolvida pelo aluno com detalhe do erro.

ATIVIDADE 4: Top Secret! Grupo ____



Criptografia com matriz inversa de terceira ordem.

Nomes dos componentes do grupo:

Matriz-chave A:

$$\begin{bmatrix} 1 & 1 & 1 \\ 3 & 2 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

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	#
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Decifre a mensagem criptografada usando a matriz-chave A acima, conforme instruções do professor:

U X J F U G F M N K W L!!!!

Mensagem decifrada:

$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} - 0 - 0 = 1 \cdot 1 = 1$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} = 1 \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} - 0 - 0 = 0 \cdot 1 = 0$

$A^{-1} = \frac{1}{1} \begin{pmatrix} 0 & 1 & -1 \\ 0 & -1 & 3 \\ 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & -2 \\ 0 & -1 & 3 \\ 1 & 0 & 1 \end{pmatrix}$

Fonte: Autora. Dados da pesquisa.

Figura 33 - Atividade 4 com detalhe do erro na resposta do aluno.

$\begin{pmatrix} 0 & 1 & -1 \\ 0 & -1 & 3 \\ 1 & 0 & 1 \end{pmatrix}$

$20 - 23 - 9 - 5 - 20 - 6 - 5 - 12 - 13 - 19 - 27 - 1$

$\begin{bmatrix} 0 & 1 & -1 \\ 0 & -1 & 3 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 20 \\ 23 \\ 9 \end{bmatrix} = \begin{matrix} 0 + 23 + (-9) = 14 \\ 0 + (-23) + 27 = 4 \\ 0 + 0 + 9 = 9 \end{matrix}$

$\begin{bmatrix} 0 & 1 & -1 \\ 0 & -1 & 3 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 20 \\ 23 \\ 6 \end{bmatrix} = \begin{matrix} 0 + 23 + (-6) = 17 \\ 0 + (-23) + 18 = -5 \\ 0 + 0 + 6 = 6 \end{matrix}$

$\begin{bmatrix} 0 & 1 & -1 \\ 0 & -1 & 3 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 20 \\ 23 \\ 11 \end{bmatrix} = \begin{matrix} 0 + 23 + (-11) = 12 \\ 0 + (-23) + 33 = 10 \\ 0 + 0 + 11 = 11 \end{matrix}$

$\begin{bmatrix} 0 & 1 & -1 \\ 0 & -1 & 3 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 20 \\ 23 \\ 11 \end{bmatrix} = \begin{matrix} 0 + 23 + (-11) = 12 \\ 0 + (-23) + 33 = 10 \\ 0 + 0 + 11 = 11 \end{matrix}$

$\begin{pmatrix} 0 & 1 & -1 \\ 0 & -1 & 3 \\ 1 & 0 & 1 \end{pmatrix} \begin{matrix} -2 \\ -1 \end{matrix}$

$20 - 23 - 9 - 5 - 20 - 6 - 5 - 12 - 13 - 19 - 27 - 1$

$\begin{bmatrix} 0 & 1 & -1 \\ 0 & -1 & 3 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 20 \\ 23 \\ 9 \end{bmatrix} = \begin{matrix} 0 + 23 + (-9) = 14 \\ 0 + (-23) + 27 = 4 \\ 0 + 0 + 9 = 9 \end{matrix}$

Fonte: Autora. Dados da pesquisa.

Durante o desenvolvimento da atividade 4, a professora percebeu que alguns alunos tinham dificuldade para calcular alguns cofatores de A, pois trocavam os elementos para calcular “o menor da entrada a_{ij} ”, conforme exemplos abaixo. No exemplo 1, foi fácil calcular, mas nos exemplos 2 e 3, eles se perderam devido à alteração dos elementos.

$$\begin{vmatrix} 1 & 2 & 0 \\ 0 & 3 & 1 \\ -1 & 2 & 1 \end{vmatrix}$$

Exemplo 1

$$\begin{vmatrix} 1 & 2 & 0 \\ 0 & 3 & 1 \\ -1 & 2 & 1 \end{vmatrix}$$

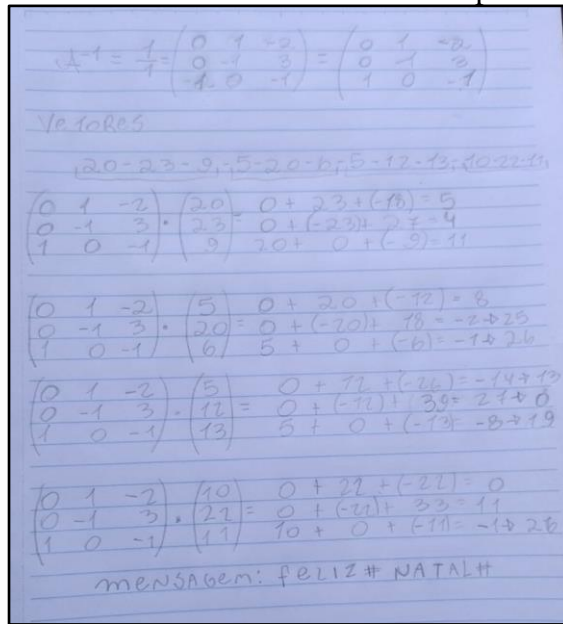
Exemplo 2

$$\begin{vmatrix} 1 & 2 & 0 \\ 0 & 3 & 1 \\ -1 & 2 & 1 \end{vmatrix}$$

Exemplo 3

Foi sugerido cobrir a linha e a coluna do respectivo elemento com uma caneta para evitar que isso acontecesse novamente. Desse modo, conseguiram concluir a atividade, conforme mostra a Figura 34.

Figura 34 - Atividade 4 corretamente resolvida pelo aluno.

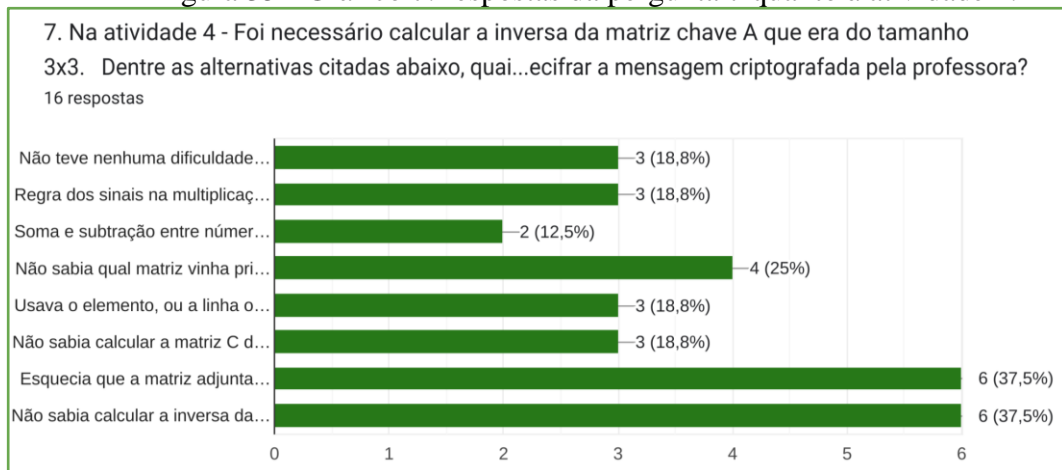


Fonte: Autora. Dados da pesquisa.

Conforme os dados no gráfico 7, na Figura 35, 18,8%, ou seja, 3 dos 16 alunos, dizem ter dificuldade de encontrar a matriz C dos cofatores de A, provavelmente devido aos fatos narrados acima e também porque para encontrar a matriz adjunta de A, foi preciso fazer a transposta da matriz C, e os alunos esqueceram disso, foram ao total 6 de 16, ou seja, 37,5%.

Logo, conclui-se que o maior problema desta atividade foi na adjunta da matriz A, motivo que desencadeou erros nos cálculos seguintes.

Figura 35 - Gráfico 7: respostas da pergunta 7 quanto à atividade 4.



Fonte: Autora. Dados da pesquisa.

Figura 36 - Pergunta 7 e suas alternativas.

7. **Na atividade 4** - Foi necessário calcular a inversa da matriz chave A que era do tamanho 3×3 .

Dentre as alternativas citadas abaixo, quais foram as dificuldades que você teve ao **decifrar** a mensagem criptografada pela professora?

Pode ser mais de uma alternativa.

Não teve nenhuma dificuldade das citadas abaixo. (Se você marcar esta alternativa não teve marcar as outras)

Regra dos sinais na multiplicação. [$(+) \times (-) = (-)$, $(-) \times (-) = (+)$, ...]

Soma e subtração entre números negativos e positivos.

Não sabia qual matriz vinha primeiro de modo que fosse possível a multiplicação entre elas.

Usava o elemento, ou a linha ou a coluna errada da matriz na hora da multiplicação.

Não sabia calcular a matriz C dos cofatores de A. (Matriz do tamanho 3×3)

Esquecia que a matriz adjunta era uma matriz C transposta. (Matriz do tamanho 3×3)

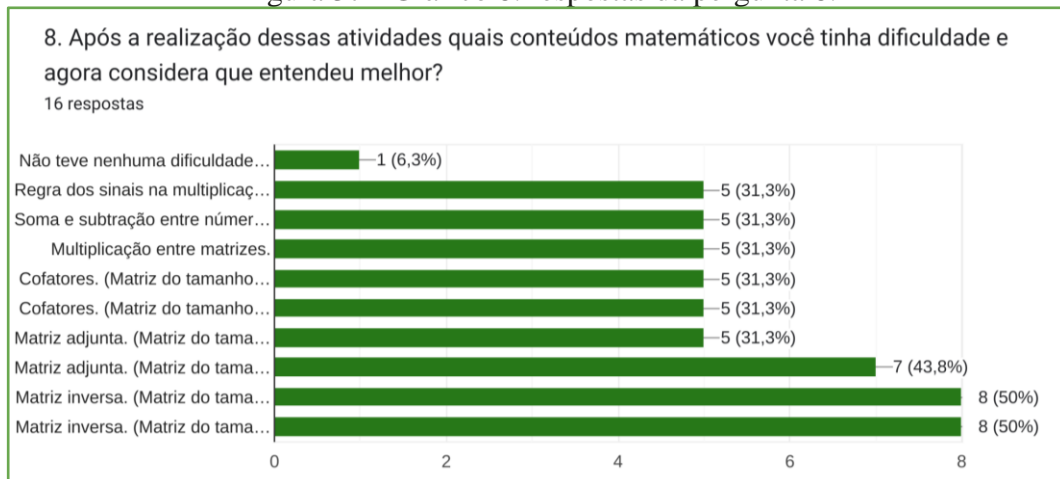
Não sabia calcular a inversa da matriz chave A. (Matriz do tamanho 3×3)

Outro:

Fonte: Autora. Dados da pesquisa.

Conforme o gráfico 8, na Figura 37, 8 dos 16 alunos, ou 62,5%, disseram ter uma melhor compreensão de como calcular multiplicação entre matrizes e calcular a matriz inversa após a conclusão da tarefa.

Figura 37 - Gráfico 8: respostas da pergunta 8.



Fonte: Autora. Dados da pesquisa.

Figura 38 - Pergunta 8 e suas alternativas.

8. Após a realização dessas atividades quais conteúdos matemáticos você tinha dificuldade e agora considera que entendeu melhor?

Pode ser mais de uma alternativa.

Não teve nenhuma dificuldade das citadas abaixo. (Se você marcar esta alternativa não teve marcar as outras também)

Regra dos sinais na multiplicação. [$(+) \times (-) = (-)$, $(-) \times (-) = (+)$, ...]

Soma e subtração entre números negativos e positivos.

Multiplicação entre matrizes.

Cofatores. (Matriz do tamanho 2x2)

Cofatores. (Matriz do tamanho 3x3)

Matriz adjunta. (Matriz do tamanho 2x2)

Matriz adjunta. (Matriz do tamanho 3x3)

Matriz inversa. (Matriz do tamanho 2x2)

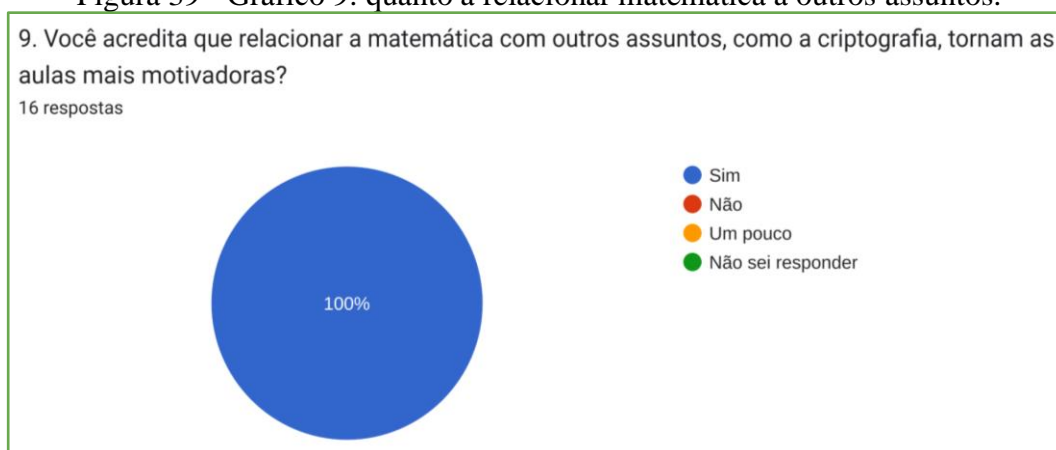
Matriz inversa. (Matriz do tamanho 3x3)

Outro: _____

Fonte: Autora. Dados da pesquisa.

Todos os entrevistados concordaram que relacionar matemática a um assunto como criptografia aumenta a motivação para aprender, como consta no gráfico 9, da Figura 39.

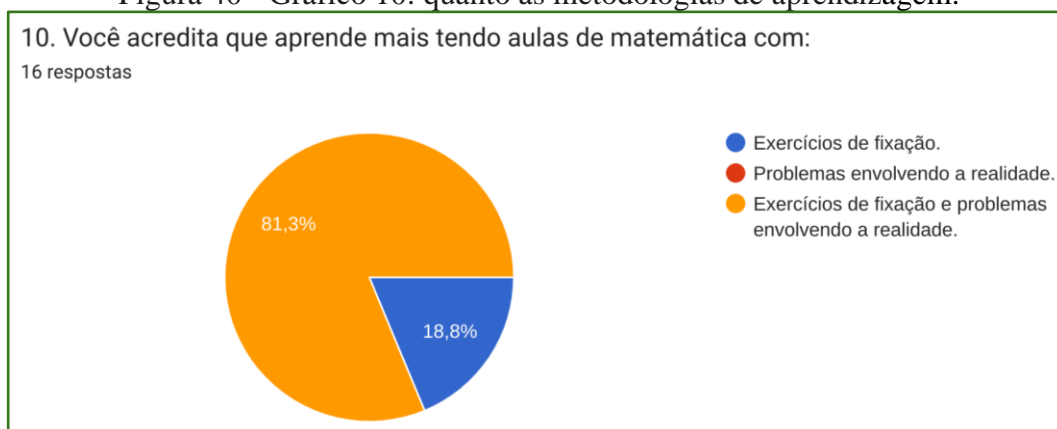
Figura 39 - Gráfico 9: quanto a relacionar matemática a outros assuntos.



Fonte: Autora. Dados da pesquisa.

No gráfico 10, da Figura 40, do total de participantes da pesquisa, 81,3% indicam que aprendem mais os conteúdos matemáticos com atividades por meio de exercícios de fixação unidos a problemas da realidade, o que nos faz perceber que nem um ou nem outro na visão desses alunos se completa sozinho. E 18,8% afirmaram que aprendem mais assistindo aulas de matemática com exercícios de fixação, ou seja, o velho e tradicional exercício.

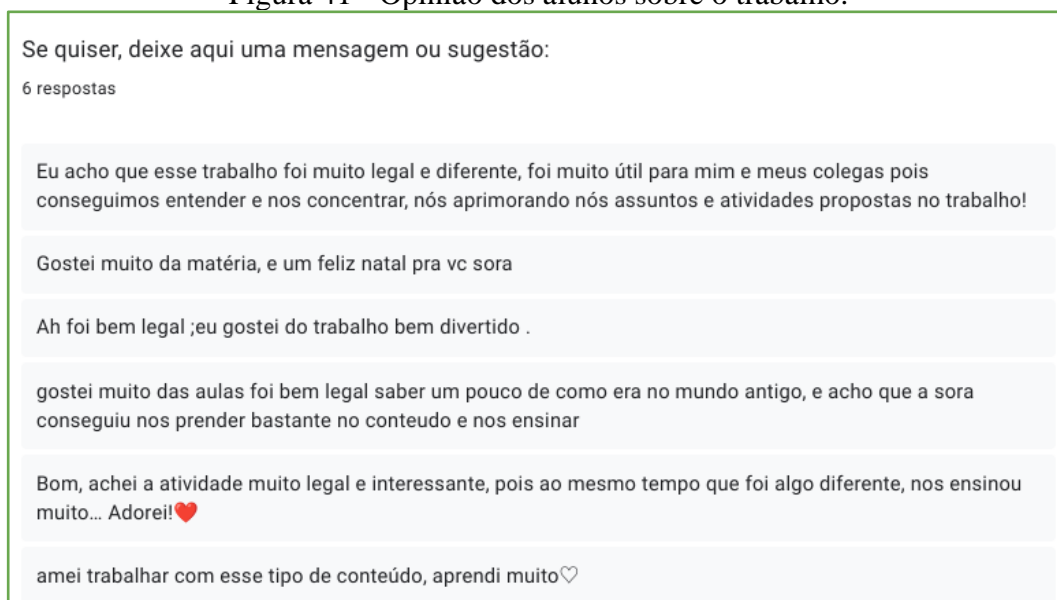
Figura 40 - Gráfico 10: quanto às metodologias de aprendizagem.



Fonte: Autora. Dados da pesquisa.

E alguns até deixaram a sua opinião, conforme mostra a Figura 41.

Figura 41 - Opinião dos alunos sobre o trabalho.



Fonte: Autora. Dados da pesquisa.

Conforme as observações da pesquisadora e da opinião dos alunos citada no questionário, foi possível notar que os alunos apresentaram uma melhora significativa em suas dificuldades matemáticas ao longo da elaboração das atividades propostas, eles admitem gostarem desse método de ensino e disseram que gostariam de ter mais aulas desse tipo.

6 CONSIDERAÇÕES FINAIS

Um dos maiores desafios na educação é fazer com que os alunos tenham interesse e aprendam novos conteúdos. Afinal, é preciso não apenas chamar a atenção deles, mas fazê-los entender a importância do conhecimento.

Para isso é preciso que os estudantes vejam qual sentido e significado tem a sua aprendizagem, considerando o conhecimento prévio que trazem do ambiente escolar e fora dele. Ao analisar as soluções e seus possíveis erros, os alunos podem aprender diferentes formas de interpretar questão por questão, alertando-os para a solução correta quando forem resolver problemas semelhantes, compreendendo e desenvolvendo o pensamento matemático correto e por vezes crítico.

A introdução de novas estratégias de ensino na sala de aula traz muitos benefícios e associa a matemática a tópicos interessantes, como criptografia, podendo facilitar a compreensão matemática, melhorando significativamente o aprendizado do aluno. O principal, é uma mudança no pensamento sobre a aprendizagem, incentivando os alunos a pensar de forma diferente, resolvendo problemas e vinculando ideias.

A criptografia é parte importante da história da matemática e pode ser um tema motivador na aprendizagem de conteúdos matemáticos. Além disso, esta pesquisa foi elaborada e aplicada com o objetivo não apenas de motivar o aprendizado matemático, mas também de estimular a consciência histórica do aluno com base no conhecimento passado.

Esses objetivos foram alcançados ao introduzirmos o tema criptografia e suas técnicas, demonstrando sua importância ao longo da história. Tornando esse tema um fator motivador no processo de ensino e aprendizagem da matemática. Ao observar, analisar e compreender o comportamento e pensamento dos sujeitos da pesquisa, durante e após o desenvolvimento da situação proposta, podemos verificar que as atividades sugeridas trouxeram benefícios para a aprendizagem.

O desenvolvimento das atividades e o *feedback* dos alunos mostraram que a criptografia é um tópico que pode ser usado para atividades educacionais. Porque motiva alunos e professores, dando sentido aos conteúdos matemáticos e beneficiando o ensino e a aprendizagem.

A criptografia tem muitos caminhos que podem ser implementados. Obviamente não podemos passar por todos eles, porque além do grande número, alguns são bastante longos e não fazem sentido neste trabalho.

Este estudo pode ser utilizado como atividade interdisciplinar por professores do ensino fundamental e médio, podendo ser elaboradas outras versões destas atividades, adaptando-as ao público-alvo, ou recorrendo a outras técnicas de encriptação, ou outros conteúdos matemáticos, tornando as aulas mais atrativas e significativas.

As competências e habilidades da BNCC, EM13MAT315 e EM13MAT405, citadas anteriormente, foram desenvolvidas nas atividades 2, 3 e 4 aplicadas neste trabalho.

Concluimos aqui o relato dessa experiência, motivados e conscientes de poder contribuir através desta abordagem para uma educação inovadora e significativa.

REFERÊNCIAS

ANTON, Howard - **Álgebra linear com aplicações** - tradução técnica: Claus Ivo Doering. – 10. Ed. – Dados eletrônicos – Porto Alegre: Bookman, 2012. Disponível em: https://www.professores.uff.br/jcolombo/wp-content/uploads/sites/124/2018/08/Algebra_Linear_com_Aplica_10_-Edi_Anton_Rorres.pdf . Acesso em: 12 out. 2022.

BEZERRA; MALAGUTTI; RODRIGUES - **Aprendendo Criptologia de Forma Divertida** (2010) - Universidade Federal da Paraíba (UFPB). Disponível em: http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf . Acesso em: 14 jan. 2023.

BRASIL. **LEI 9394**, de 20/12/1996. Diretrizes e Bases da Educação Nacional. Disponível em: <http://portal.mec.gov.br/expansao-da-rede-federal/195-secretarias-112877938/seb-educacaobasica-2007048997/12598-publicacoes-sp-265002211> . Acesso em: 10 nov. 2022.

_____. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709/2018. Disponível em: <https://www.gov.br/cidadania/pt-br/aceso-a-informacao/lgpd> . Acesso em: 04 jan. 2023.

BOZANO, Buna, Revista eletrônica. Educação e tecnologia - **O que é criptografia? Saiba mais sobre a ciência dos códigos** - crédito: Campo Grande News. 2020. Disponível em: <https://www.campograndenews.com.br/educacao-e-tecnologia/o-que-e-criptografia-saiba-mais-sobre-a-ciencia-dos-codigos> . Acesso em: 08 dez. 2022.

D'AMBROSIO, Ubiratan. **A História da Matemática: Questões Historiográficas e Políticas e Reflexivas na Educação Matemática**, in **Bicudo**, Maris Aparecida Viggiani (org.) Pesquisa em Educação Matemática: Concepções e perspectivas. São Paulo: Editora UNESP, p. 97, 1999. Disponível em: http://cattai.mat.br/site/files/ensino/unep/pfreire/docs/HistoriaDaMatematica/Ubiratan_DAmbrosio_doisTextos.pdf . Acesso em: 24 de jan. 2023.

DCODE, **Imagem**. dCode.fr. França. Disponível em: <https://www.dcode.fr/> . Acesso em: 20 nov. 2022.

DONDA, Daniel - **Criptoanálise** - 2020. Página da internet. Disponível em: <https://danieldonda.com/criptoanalise/> . Acesso em: 28 nov. 2022.

FIARRESGA, Victor Manuel Calhabrês - **Criptografia e Matemática**, 2010. 161f. Dissertação do Mestrado em Matemática para Professores - Faculdade de Ciências - Universidade de Lisboa, Lisboa - Portugal. 2010. Disponível em: <https://repositorio.ul.pt/handle/10451/3647> . Acesso em: 12 out. 2022.

FLICK, Uwe - **Introdução à pesquisa qualitativa** - Porto Alegre, 2008. Disponível em: [http://www2.fct.unesp.br/docentes/geo/necio_turra/PPGG%20%20PESQUISA%20QUALI%](http://www2.fct.unesp.br/docentes/geo/necio_turra/PPGG%20%20PESQUISA%20QUALI%20)

20PARA%20GEOGRAFIA/flick%20-%20introducao%20a%20pesq%20quali.pdf . Acesso em: 14 jan. 2023.

GANASSOLI, Ana Paula; SCHANKOSKI, Fernanda Ricardo - **Criptografia e Matemática**. 2015. 103f: i.l Dissertação do Mestrado em Matemática (PROFMAT). Departamento de Matemática, Universidade Federal do Paraná, Curitiba, PR - Brasil. Disponível em: http://www.educadores.diaadia.pr.gov.br/arquivos/File/fevereiro2016/matematica_dissertacao_s/dissertacao_fernanda_ricardo_schankoski.pdf . Acesso em: 13 out. 2022.

GIL, Antônio Carlos - **Como elaborar projetos de pesquisa** - 4. ed. - São Paulo: Atlas, 2002. Disponível em: https://moodle-ead.unipampa.edu.br/pluginfile.php/154282/mod_resource/content/1/METODOLOGIA_DO_TRABALHO_CIENTIFICO_A_J_S.pdf. Acesso em: 10 nov. 2022.

GOMES; MICHEL - **A motivação de pessoas nas organizações e suas aplicações para obtenção de resultados** - Revista Científica de Administração, n. 13, 2007. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/kC7xKUQpezmWbO8_2013-4-30-10-35-34.pdf . Acesso em: 10 nov. 2022.

MATEMÁTICA MULTIMÍDIA. Matemática na escola - **A César o que é de César!** - Aplicativo YouTube, 2012. Disponível em: <https://youtu.be/5mPAmnqlPEs> . Acesso em: 20 nov. 2022.

MATEMÁTICA MULTIMÍDIA. Matemática na escola - **O gabarito secreto** - Aplicativo YouTube, 2012. Disponível em: <https://youtu.be/Jr83wILbRaM> . Acesso em: 20 nov. 2022.

MATRIX, **Filme**, (1999-2003) - Direção: As Wachowski - Distribuído por: Warner Bros. Disponível em: <https://pt.wikipedia.org/wiki/Matrix> . Acesso em: 10 dez. 2022.

MEDEIROS; MACÊDO; PINHEIRO - **O uso da Criptografia como ferramenta motivacional nas aulas de probabilidade no Ensino Médio**, (2021) - XL CNMAC - Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS). Disponível em: <https://proceedings.sbmac.emnuvens.com.br/sbmac/article/view/135035> . Acesso em: 14 jan. 2023.

MELO, Clarissa Duarte Loureiro de - **Criptografia no Ensino Médio: uma proposta para o ensino de Matrizes** - Rio de Janeiro - 2014. Disponível em: <https://www.bdt.uerj.br:8443/bitstream/1/17533/2/Disserta%C3%A7%C3%A3o%20-%20Clarissa%20Duarte%20Loureiro%20de%20Melo%20-%202014%20-%20Completa.pdf.pdf> Acesso em: 13 jan. 2023.

O CÓDIGO DA VINCI, **Filme**, (2006) - Direção: Ron Howard - Distribuído por: Columbia Pictures. Disponível em: [https://pt.wikipedia.org/wiki/O_C%C3%B3digo_Da_Vinci_\(filme\)](https://pt.wikipedia.org/wiki/O_C%C3%B3digo_Da_Vinci_(filme)) Acesso em: 10 dez. 2022.

O JOGO DA IMITAÇÃO. **Filme**, adaptação de: Alan Turing: The Enigma. Diretor: Morten Tyldum. Distribuído por: The Weinstein Company. França, 2014. Disponível em:

https://pt.wikipedia.org/wiki/O_Jogo_da_Imita%C3%A7%C3%A3o . Acesso em: 02 dez. 2022.

OLGIN, C.A., GROENWALD, C. L. O. - **Criptografia e conteúdos de Matemática do Ensino Médio** - 2017. Disponível em:

https://www.researchgate.net/publication/319066233_Criterios_possibilidades_e_desafios_para_o_desenvolvimento_de_tematicas_no_Curriculo_de_Matematica_do_Ensino_Medio

Acesso em: 20 dez. 2022.

OLIVEIRA, Ronielton Rezende, 2012 - **Criptografia simétrica e assimétrica: os principais algoritmos de cifragem** - Artigo da revista segurança digital - Disponível em:

<https://ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf> . Acesso em: 19 dez. 2022.

OLIVEIRA, Vinícius Matos de - **Criptografia e Matemática** - Dissertação do mestrado em Matemática (PROFMAT) – Universidade Federal de Sergipe – São Cristóvão, 2020.

Disponível em: https://ri.ufs.br/bitstream/riufs/15776/2/VINICIUS_MATOS_OLIVEIRA.pdf
Acesso em: 14 jan. 2023.

PIMENTA, Andréa Lira Ribeiro - **Segurança nos contratos internacionais de compra e venda na internet: criptografia e assinatura digital** - 2004. Disponível em:

<https://repositorio.uniceub.br/jspui/bitstream/235/9411/1/20065157.pdf> . Acesso em: 12 nov. 2022.

PONTE; BROCARDO; OLIVEIRA - **Investigações matemáticas na sala de aula** – 3. ed. rev. ampl.; 2. reimp. – Belo Horizonte: Autêntica Editora, 2016. Disponível em:

<https://integrada.minhabiblioteca.com.br/reader/books/9788551301289/pageid/147> . Acesso em: 16 jan. 2023.

SINGH, Simon. **O Livro dos Códigos: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica**. Rio de Janeiro: Record, 2003. Página da internet. Disponível em:

<https://pdfcoffee.com/primeiro-capitulo-o-livro-dos-codigos-simon-singh-pdf-free.html>
Acesso em: 10 dez. 2022.

SEVERINO, Antônio Joaquim, 1941 - **Metodologia do trabalho científico** [livro eletrônico] / Antônio Joaquim Severino. – 2. ed. - São Paulo : Cortez, 2017. Disponível em:

<https://moodle-ead.unipampa.edu.br/course/view.php?id=2005#section-2> . Acesso em: 10 de nov. 2022.

SKYTALE, La - **Exposition Cryptologie** - Michel rst - França - 2016. Disponível em:

<https://youtu.be/7uq4hIV0DkU> . Acesso em: 20 nov. 2022.

TAMAROZZI, Antônio Carlos - **Codificando e decifrando mensagens** - In Revista do Professor de Matemática, 45, São Paulo: Sociedade Brasileira de Matemática, 2001.

Disponível em:

http://www.educadores.diaadia.pr.gov.br/arquivos/File/2010/veiculos_de_comunicacao/RPM/RPM45/RPM45_ . Acesso em: 22 nov. 2022.

APÊNDICE A - FOLHAS DE ATIVIDADES PARA SALA DE AULA

Atividade 1: A César, o que é de César!

Grupo _____

Mensagem cifrada e decifrada pela Cifra de Substituição.

Nome dos componentes do grupo:

“A Cifra de César”



A cifra de César é uma cifra de substituição na qual cada letra do texto original é substituída por outra letra que aparece no alfabeto abaixo dela com o deslocamento de casas. Este método de criptografia recebeu o nome do imperador romano Júlio César, que o usou para se comunicar secretamente com seus generais.

A mensagem abaixo foi criptografada pela Cifra de César, com deslocamento de 3 casas, conforme tabela:

Original	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
Codificado	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

UHIOHUR - SDEOR#QHUXGD

VH#VRX#DPDGR
 TXDQWR#PDLV#DPDGR
 PDLV#FRUUHVSRQGR#DR#DPRU
 VH#VRX#HVTXHFLGR
 GHYR#HVTXHFHU#WDPHP
 SRLV#R#DPRU#H#IHLWR#HVSHOKR
 WHP#TXH#WHU#UHIOHUR

Decifre a mensagem:

FOLHA 1

ATIVIDADE 2: Cifra-me!

Grupo

**Criptografia com multiplicação de matrizes.**

Nomes dos componentes do grupo:

--

Crie uma mensagem e codifique-a. Use a matriz-chave abaixo e tabela para conversão conforme as instruções do professor:

$$\begin{bmatrix} 7 & 17 \\ 2 & 5 \end{bmatrix}$$

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	#
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Mensagem original (de 10 a 16 letras):

--

Codificação da mensagem (com os cálculos):

--

Mensagem criptografada (apenas em letras):

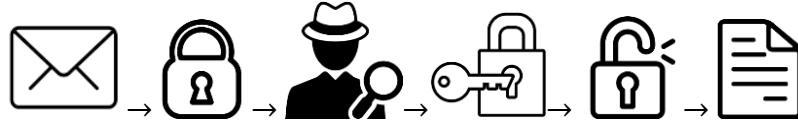
--

Escreva a mensagem criptografada e a matriz-chave em um papel e entregue para outro grupo decifrar.

FOLHA 2

ATIVIDADE 3: Decifra-me! Se for capaz!

Grupo _____



Criptografia com matriz inversa de segunda ordem.

Nomes dos componentes do grupo:

Escreva aqui a mensagem criptografada que receberam do outro grupo:

Decifre a mensagem criptografada usando a matriz-chave abaixo e tabela para conversão conforme as instruções do professor:

$$\begin{bmatrix} 7 & 17 \\ 2 & 5 \end{bmatrix}$$

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	#
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Escreva aqui a mensagem decifrada:

ATIVIDADE 4: Top Secret!

Grupo _____



Criptografia com matriz inversa de terceira ordem.

Nomes dos componentes do grupo:

Matriz-chave A:

$$\begin{bmatrix} 1 & 1 & 1 \\ 3 & 2 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

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	#
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Decifre a mensagem criptografada usando a matriz-chave A acima, conforme instruções do professor:


U X J F U G F M N K W L !!!!

Mensagem decifrada:

APÊNDICE B - QUESTIONÁRIO DA PESQUISA

Disponível para edição em:

<https://docs.google.com/forms/d/e/1FAIpQLSfzwIXk3z48pJcHxGJ4KZdevZLLpZQwT-x8eGKvtrWDgpM2Ow/viewform?usp=sf_link>



A CRIPTOGRAFIA COMO TEMA MOTIVADOR PARA O ENSINO DE MATRIZES.

Este questionário destina-se a avaliar os resultados obtidos após a conclusão das atividades feitas em sala de aula com o tema criptologia na matemática.

As questões apresentadas não têm associadas respostas corretas ou incorretas, pretendem apenas recolher opiniões pessoais.

Este questionário é anônimo e confidencial, as respostas serão utilizadas exclusivamente para fins científicos.

A sua resposta, pessoal e sincera, é muito importante!

Este questionário é parte integrante de um trabalho de investigação do Curso de Especialização em Ensino de Matemática no Ensino Médio - Matemática na Prática - da Universidade Federal do Pampa - UNIPAMPA - Campus Bagé, sob orientação da professora doutora Francieli Aparecida Vaz.

Agradeço, desde já, a sua disponibilidade e colaboração neste estudo. Estou disponível para responder a quaisquer questões no grupo do WhatsApp da turma.

DCODE, **Imagem**. dCode.fr. França. Disponível em: <https://www.dcode.fr/> . Acesso em: 20 nov. 2022.

Nome *

Sua resposta _____

1. Antes de participar destas atividades você já tinha noção do que significava criptografia e onde a encontramos no nosso cotidiano? *

Responda a esta pergunta lembrando o que você sabia, ou não, sobre criptografia antes da realização destas atividades.

Sim

Não

Sempre que você marcar a opção "outro" escreva ao lado qual ou quais são eles.

2. Se respondeu "sim" na pergunta anterior: Que lugares você já conhecia que faziam uso da criptografia? *

Pode ser mais de uma alternativa.

Respondi não na pergunta anterior.

Celular.

Fones de ouvido Bluetooth.

Transações bancárias com cartão de crédito.

Senhas de redes sociais, como WhatsApp, Facebook, Instagram entre outros.

Assinatura digital de documentos.

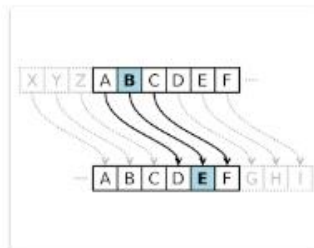
Bitcoin e criptomoedas.

Outro: _____

3. Qual dos assuntos sobre criptologia abaixo citados você achou mais interessante? *



Cítala espartana ou Bastão de Licurgo - Uma técnica de criptografia em que a mensagem era enrolada em um bastão de madeira e foi usada durante as guerras.



Cifra de César - Uma cifra romana que foi usada pelo imperador Júlio César e os seus generais durante as guerras..



A máquina Enigma - Usada pelos alemães durante a 2ª guerra mundial para cifrar mensagens.

4. Na atividade 1 - Na Cifra de César o deslocamento das letras era de 3 casas. *

O que mudaria na mensagem criptografada se o deslocamento fosse de 5 casas?

- Nada mudaria.
- Mudariam somente as letras da mensagem criptografada.
- Não seria possível fazer a criptografia com deslocamento diferente de 3 casas.
- Não sei responder.

5. **Na atividade 2** - O tamanho da matriz chave A era **2x2** e foi necessário fazer **somente a multiplicação** entre duas matrizes. *

Dentre as alternativas citadas abaixo, quais foram as dificuldades que você teve ao **cifrar** a mensagem escolhida pela sua dupla?

Pode ser mais de uma alternativa.

- Não teve nenhuma dificuldade das citadas abaixo. (Se você marcar esta alternativa não teve marcar as outras)
- Regra dos sinais na multiplicação. [(+) x (-) = (-) , (-) x (-) = (+), ...]
- Não sabia qual matriz vinha primeiro de modo que fosse possível a multiplicação entre elas.
- Usava o elemento, ou a linha ou a coluna errada da matriz na hora da multiplicação.
- Outro: _____

6. **Na atividade 3** - Foi necessário calcular a inversa da matriz chave A que era do tamanho **2x2**.

Dentre as alternativas citadas abaixo, quais foram as dificuldades que você teve ao **decifrar** a mensagem enviada pela outra dupla?

Pode ser mais de uma alternativa.

- Não teve nenhuma dificuldade das citadas abaixo. (Se você marcar esta alternativa não teve marcar as ...
- Regra dos sinais na multiplicação. [(+) x (-) = (-), (-) x (-) = (+), ...]
- Soma e subtração entre números negativos e positivos.
- Não sabia qual matriz vinha primeiro de modo que fosse possível a multiplicação entre elas.
- Usava o elemento, ou a linha ou a coluna errada da matriz na hora da multiplicação.
- Não sabia calcular a matriz C dos cofatores de A. (Matriz do tamanho 2x2)
- Esquecia que a matriz adjunta era uma matriz C transposta. (Matriz do tamanho 2x2)
- Não sabia calcular a inversa da matriz chave A. (Matriz do tamanho 2x2)
- Outros...

A questão 7 visa perceber se as dificuldades que você tinha na atividade 3 da pergunta anterior ainda continuam e quais as outras dificuldades você teve.

7. Na atividade 4 - Foi necessário calcular a inversa da matriz chave A que era do tamanho 3×3 . *

Dentre as alternativas citadas abaixo, quais foram as dificuldades que você teve ao decifrar a mensagem criptografada pela professora?

Pode ser mais de uma alternativa.

- Não teve nenhuma dificuldade das citadas abaixo. (Se você marcar esta alternativa não teve marcar as outras)
- Regra dos sinais na multiplicação. [$(+) \times (-) = (-)$, $(-) \times (-) = (+)$, ...]
- Soma e subtração entre números negativos e positivos.
- Não sabia qual matriz vinha primeiro de modo que fosse possível a multiplicação entre elas.
- Usava o elemento, ou a linha ou a coluna errada da matriz na hora da multiplicação.
- Não sabia calcular a matriz C dos cofatores de A. (Matriz do tamanho 3×3)
- Esquecia que a matriz adjunta era uma matriz C transposta. (Matriz do tamanho 3×3)
- Não sabia calcular a inversa da matriz chave A. (Matriz do tamanho 3×3)
- Outro: _____

8. Após a realização dessas atividades quais conteúdos matemáticos você tinha dificuldade e agora considera que entendeu melhor? *

Pode ser mais de uma alternativa.

- Não teve nenhuma dificuldade das citadas abaixo. (Se você marcar esta alternativa não teve marcar as outras também)
- Regra dos sinais na multiplicação. [$(+) \times (-) = (-)$, $(-) \times (-) = (+)$, ...]
- Soma e subtração entre números negativos e positivos.
- Multiplicação entre matrizes.
- Cofatores. (Matriz do tamanho 2×2)
- Cofatores. (Matriz do tamanho 3×3)
- Matriz adjunta. (Matriz do tamanho 2×2)
- Matriz adjunta. (Matriz do tamanho 3×3)
- Matriz inversa. (Matriz do tamanho 2×2)
- Matriz inversa. (Matriz do tamanho 3×3)
- Outro: _____

9. Você acredita que relacionar a matemática com outros assuntos, como a criptografia, tornam as aulas mais motivadoras? *

- Sim
- Não
- Um pouco
- Não sei responder

10. Você acredita que aprende mais tendo aulas de matemática com: *

- Exercícios de fixação.
- Problemas envolvendo a realidade.
- Exercícios de fixação e problemas envolvendo a realidade.

Se quiser, deixe aqui uma mensagem ou sugestão:

Sua resposta _____