UNIVERSIDADE DO ESTADO DE MATO GROSSO
CAMPUS DE SINOP
FACULDADE DE CIÊNCIAS EXATAS E TECNOLÓGICAS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL PROFMAT

ISAC ROSA RODRIGUES

USO DE FERRAMENTAS DE CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA PARA OS ENSINOS FUNDAMENTAL II E MÉDIO: PROPOSTAS DE ATIVIDADES

Sinop – MT
2024

ISAC ROSA RODRIGUES

USO DE FERRAMENTAS DE CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA PARA OS ENSINOS FUNDAMENTAL II E MÉDIO: PROPOSTAS DE ATIVIDADES

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, da Universidade do Estado de Mato Grosso – UNEMAT, como requisito parcial para obtenção do grau de Mestre em Matemática.

Profº. Dr. Raul Abreu de Assis
Orientador

Profª. Dra. Luciana Mafalda Elias de Assis
Co-orientadora

Sinop – MT

2024

Ficha catalográfica elaborada pela Supervisão de Bibliotecas da UNEMATCatalogação de Publicação na Fonte.
UNEMAT - Unidade padrão

Rodrigues, Isac Rosa.
Uso de ferramentas de criptografia no ensino de matemática para os Ensinos Fundamental 2 e Médio: propostas de atividades / Isac Rosa Rodrigues. - Cáceres, 2024.
112f.: il.

Universidade do Estado de Mato Grosso "Carlos Alberto Reyes Maldonado", Matemática/SNP-PROFMAT - Sinop - Mestrado Profissional, Campus Universitário De Sinop.
Orientador: Assis, Raul Abreu de.
Coorientadora: Assis, Luciana Mafalda Elias de.

1. Criptografia. 2. Propostas de Atividades. 3. Cifragem. 4. Ensino. 5. Matemática. I. Assis, Raul Abreu de. II. Assis, Luciana Mafalda Elias de. III. Título.

UNEMAT / MT-SCB CDU 51(07):003.26

ISAC ROSA RODRIGUES

USO DE FERRAMENTAS DE CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA NO ENSINO BÁSICO: PROPOSTAS DE ATIVIDADES

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional – ProfMat da Universidade do Estado de Mato Grosso/UNEMAT – Campus Universitário de Sinop, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador(a): Prof. Dr. Raul Abreu de Assis
Coorientador(a): Profa. Dra. Luciana Mafalda Elias de Assis
Aprovado em 31/08/2024

BANCA EXAMINADORA

Prof. Dr. Raul Abreu de Assis
UNEMAT – SINOP - MT

Prof. Dr. Emivan Ferreira da Silva
UNEMAT – SINOP - MT

Prof. Dr. Ricardo Robinson Campomanes Santana
UFMT - SINOP - MT

Sinop/MT
2024

À Rebeca Conceição Azevedo
e
Vanessa Rosa Rodrigues

Agradecimentos

Agradeço primeiramente a Deus pela força e consolo a mim fornecidos nas horas difíceis.

Ao meu orientador, Professor Dr. Raul Abreu de Assis, e a minha co-orientadora, Professora Luciana Mafalda Elias de Assis, pela clareza das orientações fornecidas e as importantes sugestões e pontuações indispensáveis para a elaboração deste trabalho.

Aos meus familiares, amigos e a minha namorada Rebeca pelo incentivo e companheirismo durante essa jornada.

Aos professores e colegas de classe que tive a honra e o prazer de conhecer durante essa fase da minha vida.

"O que sabemos é uma gota; o que ignoramos é um oceano".

Isaac Newton

RESUMO

Este trabalho relata uma pesquisa envolvendo estudantes do Ensino Fundamental II e do Ensino Médio do colégio Olímpio João Pissinati Guerra, no município de Sinop-MT em que são propostas atividades práticas de criptografia de mensagens simples, envolvendo conceitos matemáticos e técnicas de criptografia pautadas na Aprendizagem Significativa e na Aprendizagem Baseada em Projetos, conectando essas teorias de aprendizagem com o Ensino da Matemática e, relacionando as habilidades da BNCC com os temas trabalhados. Para tanto, apresentamos um breve resumo de conceitos matemáticos básicos necessários para o desenvolvimento das atividades propostas, além de apresentar os resultados de uma pesquisa qualitativa para investigarmos como se deu a assimilação e satisfação dos alunos a partir do que foi desenvolvido em sala de aula. As atividades foram planejadas de modo que os alunos participaram ativamente e, como resultado, geramos um produto educacional com a proposta de uma apostila contendo atividades envolvendo criptografia.

Palavras-chave: Criptografia; Proposta de atividades; Cifragem; Ensino; Matemática.

ABSTRACT

This work reports on research involving students from Elementary School II and High School at Olímpio João Pissinati Guerra School, located in the city of Sinop-MT, where practical activities of simple message encryption were proposed. These activities involved mathematical concepts and encryption techniques, based on Meaningful Learning and Project-Based Learning are proposed, connecting these learning theories with the Teaching of Mathematics and, relating BNCC skills to the topics covered. To this end, we present a brief summary of basic mathematical concepts necessary for the development of the proposed activities, in addition to presenting the results of a qualitative research to investigate how students assimilated and satisfied themselves based on what was developed in the classroom. The activities were planned so that students actively participated and, as a result, we generated an educational product with the proposal of a booklet containing activities involving cryptography.

Keywords: Cryptography; Activity proposal; Encryption; Teaching; Mathematics.

LISTA DE FIGURAS

Figura 1: Pontos essenciais no processo de aprendizagem que devem ser explorados (AUSUBEL, 1968). 17

Figura 2: Exemplo de uma mensagem cifrada utilizando a cifra de transposição. 26

Figura 3: Citales e o funcionamento da cifra do citale. 46

Figura 4: Gráfico do percentual das respostas da questão 01 do questionário. 54

Figura 5: Gráfico do percentual das respostas da questão 02 do questionário. 54

Figura 6: Gráfico do percentual das respostas da questão 03 do questionário. 55

Figura 7: Gráfico do percentual das respostas da questão 04 do questionário. 55

Figura 8: Gráfico do percentual das respostas da questão 05 do questionário. 56

Figura 9: Gráfico do percentual das respostas da questão 06 do questionário. 57

Figura 10: Gráfico do percentual das respostas da questão 07 do questionário. 57

Figura 11: Gráfico do percentual das respostas da questão 08 do questionário. 58

Figura 12: Gráfico do percentual das respostas da questão 01 do questionário. 59

Figura 13: Gráfico do percentual das respostas da questão 02 do questionário. 59

Figura 14: Gráfico do percentual das respostas da questão 03 do questionário. 60

Figura 15: Gráfico do percentual das respostas da questão 04 do questionário. 60

Figura 16: Gráfico do percentual das respostas da questão 05 do questionário. 61

Figura 17: Gráfico do percentual das respostas da questão 06 do questionário. 61

Figura 18: Gráfico do percentual das respostas da questão 07 do questionário. 62

Figura 19: Gráfico do percentual das respostas da questão 08 do questionário. 62

LISTA DE QUADROS

Quadro 1: Habilidades da BNCC que contemplam a proposta de atividades elaboradas em nossa pesquisa. 21

Quadro 2: Descrição do método de cifragem e decifragem por meio de multiplicação de matrizes. 47

SUMÁRIO

1 Introdução **15**

2 Referencial Teórico **17**

2.1 Aprendizagem Significativa 17

2.2 Aprendizagem Baseada em Projetos. 19

2.3 Ensino de Matemática 20

2.4 Habilidades da BNCC 21

3 Criptografia e Matemática: alguns fundamentos e técnicas **25**

3.1 Criptografia 25

3.1.1 Criptografia e ensino de Matemática 30

3.2 Conceitos e Ferramentas Matemáticas 31

3.2.1 Divisibilidade e Divisão Euclidiana 31

3.2.2 Funções 34

3.2.3 Matrizes 36

3.2.4 Análise Combinatória 41

3.2.5 Estatística 44

4 Atividades Aplicadas e suas Experiências no Ensino Fundamental II e no Ensino Médio **47**

4.1 O Citale. 47

4.2 Multiplicação de Matrizes 48

4.3 Atividades Propostas no 9º Ano do Ensino Fundamental II 50

4.4 Atividades Propostas no 2º Ano do Ensino Médio 51

4.5 Algumas Reflexões e Relatos sobre as Atividades 52

5 Discussões e Conclusões. **55**

5.1 Resultados e Análise do Questionário Aplicado nas Turmas do 9º ano do Ensino Fundamental II 55

5.2 Resultados e Análise do Questionário Aplicado na Turma do 2º ano do Ensino Médio 60

5.3 Reflexões Finais 65

Referências Bibliográficas 66

Apêndice **69**

Apêndice 1: Apostila de Propostas de Atividades para Aulas de Matemática no Ensino Fundamental II e no Ensino Médio Baseadas em Técnicas de Criptografia 66

Anexo **108**

Anexo I: Questionário elaborado para o 9º ano do Ensino Fundamental II e para o 2º ano do Ensino Médio, como parte da avaliação das atividades práticas em sala de aula. 108

1. INTRODUÇÃO

A presença da matemática em nosso cotidiano é inegável. Ela permeia as atividades mais sutis de nosso dia a dia, desde a gestão de finanças pessoais até a resolução de problemas práticos, como calcular trajetórias ou dimensionar receitas na cozinha. No entanto, a maneira como a Matemática é tradicionalmente ensinada nas escolas frequentemente diverge dessa realidade cotidiana, levantando questões pertinentes sobre a sua eficácia na formação dos alunos.

Este estudo busca abordar temas como aprendizagem significativa e ensino de Matemática no contexto da elaboração de atividades que possam ser realizadas em sala no Ensino Básico, mais precisamente, no Ensino Fundamental II e no Ensino Médio (especificamente em turmas do 9º ano do Ensino Fundamental II ao 2º ano do Ensino Médio).

O distanciamento entre a aplicação prática da Matemática e seu ensino formal tem sido objeto de estudo e reflexão em diversas obras acadêmicas. Autores como Paulo Freire (1973) e Deborah Ball (1990) exploraram as lacunas entre a vivência matemática do indivíduo e o currículo escolar, destacando a importância de conectar os conhecimentos matemáticos com as experiências vivenciadas no dia a dia pelo aluno. Essa desconexão entre o que a Matemática é na prática, e como é apresentada na sala de aula, pode resultar em uma compreensão limitada e no desinteresse dos estudantes pela disciplina (BOALER, 2016).

Este estudo visa desenvolver uma apostila contendo propostas de atividades de matemática para o Ensino Fundamental II e Ensino Médio, com base em técnicas de criptografia e criptoanálise.

O foco é oferecer material de apoio para professores do Ensino Fundamental II e do Ensino Médio, a fim de possibilitar uma aproximação entre a matemática presente no dia a dia e sua abordagem pedagógica, propondo estratégias que aproximem os conceitos matemáticos presentes no currículo escolar da aplicação prática dos mesmos.

A pesquisa se apoia em obras de referência sobre metodologia do ensino de matemática e literatura de divulgação matemática centrada no tema criptografia, com o propósito de contribuir para o ensino de matemática, buscando torná-lo mais contextualizado e significativo para os estudantes.

Este trabalho está dividido em quatro Capítulos. O Capítulo 1 trata-se desta Introdução. No Capítulo 2, apresentamos nossos referenciais teóricos fazendo uma breve revisão sobre Aprendizagem Significativa e Aprendizagem Baseada em Projetos (ABP) conectando essas teorias com o Ensino da Matemática e, relacionando as habilidades da BNCC com os temas trabalhados na proposta de atividades que elaboramos para o Ensino Fundamental II e o Ensino Médio. No Capítulo 3, apresentamos um resumo sobre criptografia e também, os conceitos matemáticos básicos necessários para a nossa proposta de atividades. No Capítulo 4, fazemos um relato de experiência em como se deu a aplicação em sala de aula. Finalmente, no capítulo 5, fazemos uma discussão dos resultados obtidos no Capítulo 4 e apresentamos uma conclusão geral do trabalho e perspectivas para novos trabalhos a partir do que foi desenvolvido nesta pesquisa, buscando instigar os alunos de maneira motivadora.

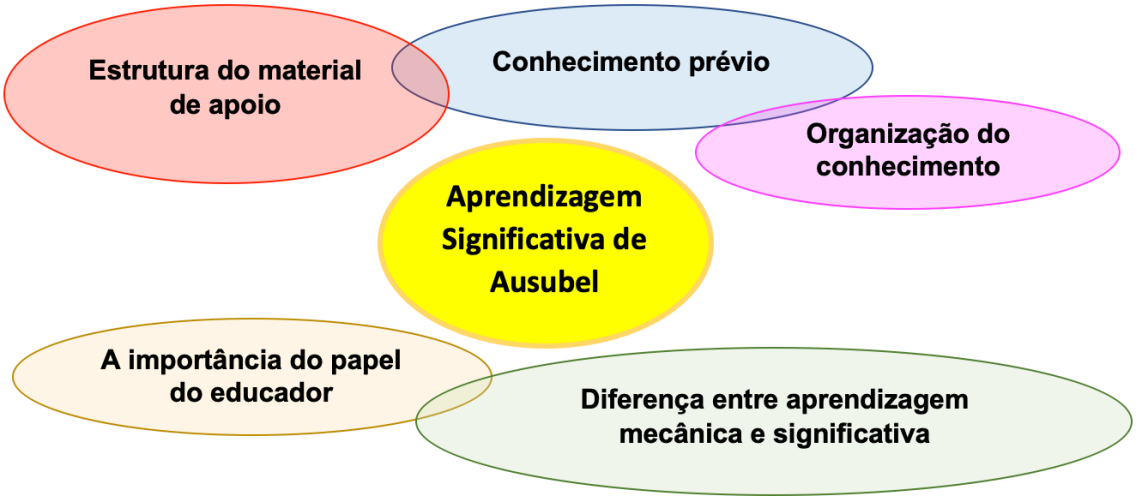
2. REFERENCIAL TEÓRICO

Neste Capítulo, faremos uma breve revisão sobre Aprendizagem Significativa e Aprendizagem Baseada em Projetos (ABP) que servirão para fundamentar a proposta de atividades presente no apêndice deste trabalho. Além disso, apresentamos as habilidades da BNCC relacionando-as com os conteúdos matemáticos abordados em nossa proposta de atividades que foram elaboradas especialmente para os alunos do 9º ano do Ensino Fundamental II e do 2º ano do Ensino Médio.

2.1 Aprendizagem significativa

A Aprendizagem Significativa é uma teoria da aprendizagem proposta pelo psicólogo educacional David Ausubel, que enfatiza a importância em conectar novos conhecimentos com o conhecimento prévio do aprendiz (AUSUBEL, 1982). De acordo com Ausubel (1968), existem alguns pontos essenciais no processo de aprendizagem que devem ser explorados, na Figura 1, fazemos um esboço de tais pontos, os quais detalhamos em seguida.

Figura 1: Pontos essenciais no processo de aprendizagem que devem ser explorados (AUSUBEL, 1968).



Fonte: o autor.

- Conhecimento prévio: Para Ausubel a aprendizagem ocorre quando o novo conhecimento é ancorado em conceitos, ideias e informações já

existentes ou conhecidas. Ele chamou o conhecimento prévio de "subsunçor" e classificou-o como fundamental para uma aprendizagem significativa.

- Organização do conhecimento: O processo de ensino-aprendizagem é efetivo quando se considera a importância de organizar o conhecimento de maneira hierárquica é essencial para que o aprendizado comece com conceitos mais gerais e, em seguida, progrida para conceitos mais específicos. Esse processo de organização facilita a compreensão e a retenção do novo conhecimento.

- Diferença entre aprendizagem mecânica e aprendizagem significativa: A existência de diferenças entre essas duas modalidades, devem ser observadas e reconhecidas pelos educadores. Na aprendizagem mecânica, o conhecimento é memorizado de forma superficial, muitas vezes sem compreensão real, e pode ser esquecido rapidamente após o aprendizado. Por outro lado, na aprendizagem significativa, os novos conceitos são incorporados de forma lógica e integrados ao conhecimento prévio do aprendiz. Isso torna o aprendizado mais prático e útil, uma vez que o aluno é capaz de aplicar o conhecimento em contextos diversos.

- Estrutura do material de apoio: Para promover uma aprendizagem significativa, Ausubel enfatiza a de que, ao se projetar materiais de apoio, estes devem ser claros e organizados, respeitando a já citada hierarquia na organização do conhecimento em estudo, e cuja finalidade primordial consiste em ajudar os alunos a conectar o novo conhecimento com o que já sabem. Ele sugere o uso de exemplos, analogias e comparações para facilitar a compreensão e a integração do novo material.

- A importância do papel do educador: Finalmente, Ausubel argumenta que os educadores desempenham um papel fundamental na promoção da aprendizagem significativa. Eles devem auxiliar os alunos a identificar

e organizar seus conhecimentos prévios, criar conexões relevantes entre os conceitos e cultivar a reflexão. Além disso, os educadores devem adaptar suas abordagens de ensino de acordo com as necessidades e níveis de compreensão de cada aluno.

De maneira resumida, a Aprendizagem Significativa destaca a importância de se construir o conhecimento a partir do que já sabemos, em oposição à mera memorização de fatos isolados. Essa abordagem visa possibilitar ao aprendiz uma análise crítica e organizada dos conceitos estudados, além da capacidade de deduzir e demonstrar conceitos novos e relações a partir do conhecimento que já foi incorporado, criando assim uma base sólida de compreensão que os alunos possam aplicar em diversas situações, promovendo uma aprendizagem mais rigorosa e útil.

2.2 Aprendizagem baseada em projetos

A Aprendizagem Baseada em Projetos (ABP) é uma abordagem pedagógica que tem ganhado destaque no ambiente educacional contemporâneo. Segundo Thomas (2000), a ABP é um método que possibilita aos estudantes explorar questões complexas, muitas vezes interdisciplinares, por meio da elaboração e execução de projetos, promovendo uma aprendizagem mais contextualizada e significativa. Nesse contexto, Dewey (1979) enfatiza que o aprendizado por meio de projetos permite aos alunos não apenas adquirir conhecimento, mas também desenvolver habilidades de resolução de problemas, colaboração e pensamento crítico. Ele destaca a importância de experiências práticas e concretas para a construção do conhecimento, apontando que a realização de projetos envolve os alunos em um processo ativo de aprendizagem.

Além disso, Vygotsky (1978) desenvolveu o conceito de Zona de Desenvolvimento Proximal (ZDP), que descreve a diferença entre o que um aluno pode fazer sozinho e o que pode fazer com a ajuda de outras pessoas. A ABP promove exatamente esse tipo de interação social e colaboração, ao incentivar os alunos a resolver problemas de forma ativa e colaborativa, com o apoio de colegas ou facilitadores. Dessa forma a ABP oferece oportunidades para a construção do conhecimento em um contexto social, onde os alunos

interagem, colaboram e negociam significados, contribuindo para o desenvolvimento cognitivo e socioemocional.

Uma implementação bem sucedida da ABP requer não apenas a definição de projetos pertinentes ao conteúdo e relevantes para os alunos, mas também um papel ativo do professor como facilitador do processo (BLUMENFELD *et al.*, 1991). O professor assume um papel de guia, fornecendo suporte, orientação e feedback aos alunos durante todo o desenvolvimento do projeto.

No entanto, é importante destacar que a eficácia da ABP está diretamente ligada ao planejamento cuidadoso, à avaliação adequada e à integração dos projetos ao currículo escolar (CHEFE, 2018). A criação de projetos alinhados aos objetivos de aprendizagem e a adaptação às necessidades dos alunos são aspectos cruciais para o sucesso dessa abordagem. Levando esses aspectos em consideração e aliando-os ao fato de que projetos costumam envolver diferentes áreas do saber, a ABP pode ser aplicada para se tratar não apenas conteúdos de disciplinas isoladas do currículo, mas também os chamados temas transversais definidos pela BNCC como essenciais de serem abordados no Ensino Fundamental II e no Ensino Médio.

2.3 Ensino de Matemática

O Ensino de Matemática é um desafio constante para educadores, exigindo estratégias e intervenções pedagógicas eficazes para promover uma aprendizagem significativa e engajadora. Segundo a Base Nacional Curricular Comum (BNCC) a Matemática, como disciplina escolar, deve ser apresentada de forma contextualizada, estimulando a compreensão e a aplicação dos conceitos no cotidiano dos alunos como ferramentas para a compreensão dos mundos mental, social e natural (BRASIL, 2017).

Para atender a essa demanda, é essencial adotar metodologias que estimulem a participação ativa dos estudantes no processo de aprendizagem. Nesse sentido, Oliveira (2016) destaca a importância de estratégias como a resolução de problemas, o uso de jogos educativos e a manipulação de materiais concretos como meios experimentais para desenvolver o raciocínio lógico-matemático dos alunos. A resolução de problemas, de acordo com

Fiorentini e Lorenzato (2006), permite aos alunos aplicar os conhecimentos matemáticos em situações reais, estimulando o pensamento crítico e a busca por soluções. Além disso, o uso de jogos educativos, conforme recomendações de D'ambrósio (1996), proporciona um ambiente lúdico e motivador, promovendo uma aprendizagem por meio do prazer e da interação social.

A manipulação de materiais concretos, como defendido por Castellar (2014), é uma estratégia eficaz para a compreensão de conceitos abstratos. O contato direto com objetos tangíveis possibilita aos alunos uma visualização mais clara e uma compreensão mais profunda dos conceitos matemáticos. Nesse contexto, o conceito de materiais concretos pode ser generalizado para o de situações concretas nas quais não necessariamente existe um objeto físico a ser medido ou de algum modo quantificado por meios matemáticos, mas sim situações onde se faz necessária uma análise quantitativa, organizada e logicamente fundamentada para a resolução de algum problema característico da situação, podendo então ser feito o uso de ferramentas matemáticas para a compreensão da natureza da situação, dedução de suas propriedades, elaboração de hipóteses e de algoritmos para resolução de problemas.

2.4 Habilidades da BNCC

As atividades propostas neste trabalho estão relacionadas com algumas habilidades da Base Nacional Comum Curricular (BNCC) para os Ensinos Fundamental II e Médio na área de Matemática e suas tecnologias. A seguir, apresentamos no Quadro 1, algumas das habilidades da BNCC contempladas e como elas se relacionam com a proposta de atividades elaboradas em nossa pesquisa.

Quadro 1: Habilidades da BNCC que contemplam a proposta de atividades elaboradas em nossa pesquisa.

Habilidades da BNCC	Relação com a proposta de atividades
(EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.	Os conceitos de múltiplos e de divisores estão fortemente relacionados com a divisão euclidiana na forma de quociente e resto. O caso particular em que o resto de uma divisão é zero pode ser utilizado para definir tais conceitos. Mais adiante,

	nas atividades de criptografia utilizando um *citale*, veremos que os múltiplos e divisores aparecem naturalmente como uma forma de técnica de decifragem.
(EF09MA03) Efetuar cálculos com números reais, inclusive potências com expoentes fracionários.	As diversas atividades propostas envolvem a realização das operações básicas com números reais, mesmo que a fim de focar nas ideias utilizadas e não nas operações os exemplos foram elaborados em sua maioria utilizando números inteiros.
(EM13MAT102) Analisar tabelas, gráficos e amostras de pesquisas estatísticas apresentadas em relatórios divulgados por diferentes meios de comunicação, identificando, quando for o caso, inadequações que possam induzir a erros de interpretação, como escalas e amostras não apropriadas.	A habilidade de criar, analisar e manipular gráficos e tabelas é frequentemente necessária para lidar com as transformações e permutações pelas quais os caracteres de um texto passam durante uma cifragem.
(EM13MAT106) Identificar situações da vida cotidiana nas quais seja necessário fazer escolhas levando-se em conta os riscos probabilísticos (usar este ou aquele método contraceptivo, optar por um tratamento médico em detrimento de outro etc.).	Os processos de contagem utilizados nas atividades relacionadas à análise combinatória são ferramentas essenciais para determinar o número de eventos possíveis em um espaço amostral a ser utilizado no cálculo de probabilidades.
(EM13MAT301) Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, com ou sem apoio de tecnologias digitais.	Sistemas lineares de equações podem ser representados na forma matricial e a solução pode ser obtida através de operações matriciais, entre elas o cálculo do determinante da matriz que também é utilizado na cifragem por multiplicação de matrizes para determinar se uma matriz é invertível ou não.
(EM13MAT302) Construir modelos empregando as funções polinomiais de 1º ou 2º graus, para resolver problemas	Na atividade da cifragem por citale podemos modelar a posição de um caractere do texto original no texto cifrado como função da sua posição no

em contextos diversos, com ou sem apoio de tecnologias digitais.	texto original através de uma função afim onde o número de lados do citale é o coeficiente angular e a posição de uma letra arbitrária no texto cifrado através da qual indicamos a posição dos outros caracteres é o coeficiente linear.
(EM13MAT310) Resolver e elaborar problemas de contagem envolvendo agrupamentos ordenáveis ou não de elementos, por meio dos princípios multiplicativo e aditivo, recorrendo a estratégias diversas, como o diagrama de árvore.	As técnicas de contagem e aplicação dos princípios aditivo e multiplicativo são ferramentas usadas para definir o número de cifras distintas que podemos obter ao aplicar determinado tipo de cifragem.
(EM13MAT311) Identificar e descrever o espaço amostral de eventos aleatórios, realizando contagem das possibilidades, para resolver e elaborar problemas que envolvem o cálculo da probabilidade.	A definição de espaços amostrais e o cálculo de probabilidades são necessários para deduzir um possível caractere ou conjunto de caracteres em determinada posição de um texto cifrado comparando com a probabilidade de o mesmo aparecer nessa posição em textos da língua na qual o texto original foi escrito.
(EM13MAT315) Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.	Apesar de não haver neste trabalho um foco em registrar algoritmos, em cada método de cifragem existe algum algoritmo, ou ao menos um caminho geral para a decifragem.
(EM13MAT406) Construir e interpretar tabelas e gráficos de frequências com base em dados obtidos em pesquisas por amostras estatísticas, incluindo ou não o uso de *softwares* que inter-relacionem estatística, geometria e álgebra.	A construção de tabelas de frequências para letras e palavras de determinado idioma é uma ferramenta essencial para as decifragens por análise de frequência.
(EM13MAT507) Identificar e associar progressões aritméticas (PA) a funções afins de domínios discretos, para análise de propriedades,	Na cifragem por citale o número de lados do citale utilizado para cifrar um texto define a razão de um conjunto de progressões aritméticas que podem ser usadas para identificar quais números

dedução de algumas fórmulas e resolução de problemas.	deixam o mesmo resto ao serem divididos por um mesmo divisor.

Fonte: o autor.

Essas habilidades da BNCC evidenciam a relevância e a aplicabilidade das atividades propostas, pois estão diretamente relacionadas à resolução de problemas, interpretação de situações-problema, aplicação de conceitos matemáticos em diferentes contextos e desenvolvimento do pensamento crítico e analítico dos alunos. Além das habilidades citadas, em geral, as habilidades da BNCC concentram-se na capacidade de resolução de problemas e aplicações práticas da matemática, o que evidentemente é abordado neste trabalho.

3. CRIPTOGRAFIA E MATEMÁTICA: ALGUNS FUNDAMENTOS E TÉCNICAS

Neste Capítulo, apresentamos um breve resumo sobre Criptografia para que seja possível compreendê-la dentro do contexto de nossa pesquisa, incluindo os principais conceitos matemáticos necessários para sua assimilação.

3.1 Criptografia

A criptografia, ao longo da história humana, desempenhou um papel crucial na proteção de informações sensíveis e na garantia da segurança de comunicações em diversos contextos. Sendo a criptografia o tema de interesse deste trabalho, no qual se pretende explorar a matemática da mesma, faremos uma revisão do tema, baseados na obra “O livro dos códigos”, do autor Simon Singh (SINGH, 2023). A seguir, apresentamos um breve relato de conceitos e definições relacionados ao campo da criptografia, sua evolução, justificativa de uso e alguns fatos históricos relacionados.

O livro de Singh (2023) oferece uma exploração detalhada das raízes da criptografia, destacando suas origens nas antigas civilizações, examinando como diferentes sociedades desenvolveram e utilizaram métodos de codificação para proteger mensagens e segredos importantes. Porém, antes de definir com precisão o que podemos chamar de criptografia, temos de diferenciá-la de outras técnicas de proteção de informações, a principal delas é a esteganografia, que consiste em ocultar uma mensagem em si sem alterar as informações da mesma.

Como exemplos, podemos citar qualquer técnica que envolva esconder a mensagem em si. Singh (2023) cita que na antiguidade grega há dois registros de uso da esteganografia, em um, uma mensagem foi escrita em tábuas de madeira que foram cobertas com cera e em seguida enviadas ao destinatário, na época, tábuas cobertas de cera eram usadas para escrever, mas sobre a cera, e, portanto, a mensagem nessa ocasião passou

despercebida pois as tábuas aparentavam estar “novas”, ou seja, não utilizadas.

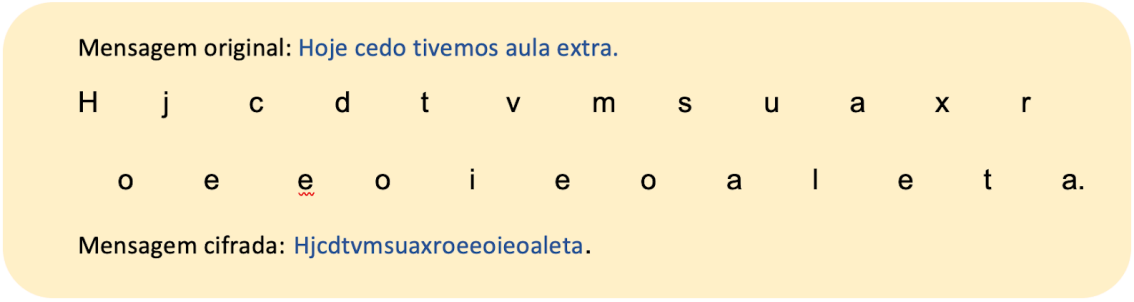
O outro registro trata de uma mensagem tatuada no couro cabeludo de um homem cujo cabelo havia sido raspado, por ter sido escrita com muita antecedência em relação ao momento em que deveria ser recebida, houve tempo suficiente para que o cabelo do “mensageiro” crescesse e ele pudesse viajar com a mensagem sem levantar qualquer suspeita, ao chegar ao destino, raspou novamente o cabelo e mostrou a mensagem ao destinatário.

Outros métodos de esteganografia são citados como o uso de uma tinta especial sobre um ovo cozido, de modo que tal tinta penetra a casca e grava a mensagem sobre a clara endurecida do ovo, para ler a mensagem basta retirar a casca.

O ponto fraco da esteganografia é que se apesar de escondida, se a mensagem for descoberta, seu significado é claro, por isso houve também a criação e desenvolvimento da criptografia, cuja função é alterar a mensagem enviada de uma forma previamente conhecida pelo destinatário de modo que possíveis interceptadores não sejam capazes de lê-la, caso tenham acesso a mesma, o ato de alterar uma mensagem é chamado de encriptação ou cifragem. Dessa forma, duas técnicas muito utilizadas em cifragem são a transposição e a substituição, que exemplificaremos a seguir.

Nas cifras de transposição, os caracteres de uma mensagem são trocados de lugar uns com os outros segundo um certo padrão, essa troca é chamada de rearranjo e o texto obtido é um anagrama do original. Um exemplo simples de cifra de transposição consiste em distribuir alternadamente os caracteres de uma mensagem em duas linhas (ou mais) e depois obter a mensagem cifrada escrevendo seguidamente os caracteres da primeira linha e após estes os da segunda, conforme ilustrado da Figura 2.

Figura 2: Exemplo de uma mensagem cifrada utilizando a cifra de transposição.



Fonte: o autor.

Enquanto as cifras de transposição preservam os caracteres da mensagem mudando suas posições, a cifragem por substituição consiste em trocar cada caractere da mensagem por um outro previamente definido por um padrão que chamamos de chave. Dessa forma, uma cifra por substituição preserva a posição de um caractere mas altera sua “identidade”, muitas das cifras de substituição consistem na troca das letras da mensagem através da relação entre o alfabeto padrão da linguagem em que a mensagem é escrita e um alfabeto onde as letras estejam em posições diferentes, chamado de alfabeto cifrado.

Uma das cifras desse tipo mais antigas abordadas pelo autor é a cifra de César, atribuída ao próprio líder militar romano Júlio César. Esta técnica simples de substituição de letras foi um dos primeiros exemplos documentados desse tipo de criptografia e foi utilizada para codificar comunicações militares durante campanhas importantes. É dito que César trocava cada letra de uma mensagem por uma outra que estivesse três casas à frente dela no alfabeto, dessa maneira o alfabeto cifrado é obtido simplesmente deslocando o alfabeto original por três casas. É evidente que qualquer deslocamento entre 1 e 25 casas resultará em um alfabeto cifrado distinto, não sendo o deslocamento de três casas um padrão absoluto.

Apesar dessa divisão das cifras em dois grupos, é possível também criar cifras que se utilizem dos dois métodos simultaneamente. Um exemplo seria uma cifra que se utiliza de um alfabeto cifrado, criado pelo deslocamento em certa quantidade de casas (substituição) do alfabeto original, e que é aplicado para substituir os caracteres não do texto original, mas sim, de um rearranjo deste (transposição).

No livro, Singh (2023) explora o contexto histórico em que diversas cifras foram desenvolvidas, aprimoradas e utilizadas, destacando sua importância em períodos de conflitos militares, diplomáticos e comerciais. Além do que já foi exposto, durante a Idade Média, por exemplo, a criptografia desempenhou um papel vital nas comunicações entre reinos rivais, grupos separatistas que planejavam golpes de estado e até mesmo entre membros do clero.

Durante a Renascença, com o aumento do comércio e das trocas culturais, a necessidade de proteger informações confidenciais relacionadas a métodos e técnicas de produção tornou-se ainda mais presente. É fácil perceber que essas mesmas razões são motivadoras no mundo atual, inclusive com uma importância ainda maior devido à grande quantidade de informação que é transmitida a todo momento.

Antes de chegar, entretanto, nos dias atuais e na importância da criptografia na era da internet, o autor descreve os significativos avanços testemunhados pela área da criptografia no Século XX, impulsionados pelo rápido desenvolvimento da tecnologia e das comunicações. Nas primeiras décadas do Século passado, as mensagens enviadas via radiofrequência podiam ser interceptadas por qualquer um que tivesse o aparelho radioreceptor disponível e, portanto, o papel da criptografia foi crucial nos contextos militares.

A Segunda Guerra Mundial, por exemplo, foi um período marcante para a evolução da criptografia. As cifras, antes, criadas de modo mais “manual” agora eram obtidas rapidamente com o uso de máquinas de cifragem complexas, como a Enigma, criada pelos alemães.

Esta, e outras máquinas de cifragem faziam o trabalho de transpor e substituir caracteres de uma mensagem instantaneamente através de seus mecanismos internos. Por serem, em sua maioria, máquinas eletromecânicas, possuíam diversos parâmetros capazes de alterar a cifra obtida, sendo possível assim não apenas criar cifras extremamente difíceis de serem quebradas mas também evitar a repetição no uso de determinada cifra, fazendo com que qualquer avanço obtido por um interceptador em determinada mensagem não seja aplicável em mensagens seguintes, nas quais os parâmetros da máquina seriam alterados.

Essas máquinas eram desenvolvidas de modo a desfazer a cifragem caso a mensagem cifrada fosse introduzida na máquina, desse modo emissário

e destinatário poderiam se comunicar com relativa segurança desde que tivessem posse de um mesmo modelo de máquina e combinassem previamente a regulagem que utilizariam para os parâmetros. Descobrir o padrão de transposição e substituição empregado por máquinas de cifragem é algo praticamente impossível para uma mente humana e a limitada quantidade de tentativas de “hipóteses” de possíveis padrões que somos capazes de testar em certo período de tempo.

Para quebrar a criptografia dessas máquinas, foi necessário que outras máquinas fossem desenvolvidas, máquinas essas capazes de realizar muitos testes através de cálculos matemáticos em pouco tempo, e também foi necessário que essas máquinas fossem programáveis, ou seja, capazes de realizar tarefas ou aplicar algoritmos distintos conforme as alterações determinadas por comandos de seus operadores. Estas últimas foram as primeiras calculadoras programáveis, criadas para decifrar mensagens secretas e que, hoje, chamamos de computadores.

Além das aplicações militares, o livro de Singh examina a relevância da criptografia em contextos civis, como a proteção de informações pessoais e financeiras na era digital. Com o advento da Internet e a proliferação de dados digitais, a criptografia tornou-se uma ferramenta essencial para garantir a privacidade e a segurança de informações sensíveis transmitidas eletronicamente. Isso foi pensado logo no início da popularização dos computadores e, principalmente, da internet e da comunicação por e-mails.

Para garantir a segurança no ambiente digital, era necessário algum tipo de criptografia resistente aos ataques dos computadores atuais, muito mais potentes em termos de capacidade de processamento do que aqueles desenvolvidos durante a segunda guerra mundial e usados para decifrar as mensagens criadas pelas máquinas de cifragem. Era necessário que uma cifra muito forte fosse implementada pelos próprios computadores e funcionasse de tal modo que nem outro computador pudesse quebrá-la em tempo hábil. Porém, tal cifra só faria sentido se o destinatário fosse capaz de decifrá-la, ou seja, uma chave deveria ser previamente combinada entre remetente e destinatário.

Como o volume de informações trocadas na internet era muito alto desde o início de sua utilização, era evidente que a necessidade da troca de

chaves seria um problema muito grave, tornando a criptografia das mensagens inviável.

Uma solução desenvolvida para isso foi o chamado sistema de criptografia, onde não há apenas uma chave e sim duas. Uma é chamada de chave pública, é acessível a qualquer computador conectado à internet, enquanto outra é chamada de chave privada, e é de propriedade particular do computador do emissário. Através de alguns algoritmos específicos e com a utilização das chaves pública e privada é possível trocar informações na internet com segurança, como somos capazes de fazer atualmente.

Entre as técnicas de criptografia assimétrica, uma das mais utilizadas na internet é a chamada criptografia RSA, nomeada assim em homenagem aos seus criadores. Nesse tipo de criptografia, operações numéricas baseadas em propriedades matemáticas estudadas em Teoria dos Números são utilizadas para criar um método muito eficaz de cifragem com uso de uma chave pública e uma privada, permitindo que a comunicação seja realizada adequadamente.

3.1.1 Criptografia e ensino de Matemática

O uso da criptografia no ensino de matemática tem se mostrado uma metodologia promissora para motivar os alunos e tornar o processo de aprendizagem mais interativo e aplicável. A criptografia é tradicionalmente associada à segurança da informação, mas no contexto educacional, seu potencial vai além, permitindo que os alunos aprendam conceitos matemáticos de forma prática, como em problemas de codificação e decodificação de mensagens.

No ensino médio, a criptografia tem sido utilizada como ferramenta didática, especialmente em disciplinas como combinatória e álgebra. Um estudo empírico realizado por Vidal et al. (2022) aplicou uma sequência didática para ensinar análise combinatória através da criptografia. A sequência envolveu 26 horas de aula e foi implementada em uma turma de 22 alunos do segundo ano do ensino médio. A proposta incluiu técnicas de contagem e conceitos criptográficos, como a cifra de César e a criptografia binária, além de conexões com a criptografia apresentada no filme O Código Da Vinci. Pontes et al. (2022) exploraram o uso de funções polinomiais na criptografia como uma

prática pedagógica inovadora para alunos do final do ensino fundamental e início do ensino médio. A abordagem consistiu em codificar e decodificar mensagens usando polinômios, o que permite que os alunos compreendam melhor a álgebra e suas aplicações em situações reais, promovendo maior engajamento e motivação para o aprendizado de matemática.

Outro exemplo de integração da criptografia no ensino de matemática pode ser observado no uso de criptografia para ensinar matrizes no ensino médio. A proposta de usar matrizes como parte de um sistema criptográfico não só auxilia na compreensão do conceito, como também fornece uma aplicação concreta para uma área abstrata da matemática (MELO, 2014).

Além das abordagens tradicionais, a criptografia também se beneficia do uso de tecnologias digitais como ferramentas complementares no ensino. Da Silva et al. (2022) propõem que o uso de softwares criptográficos aliados à tecnologia digital pode aumentar o interesse dos alunos pela matemática, proporcionando uma interface interativa para aprender conceitos matemáticos complexos de maneira mais intuitiva e acessível.

O ensino de matemática por meio da criptografia oferece um meio mais dinâmico de abordar conteúdos matemáticos muitas vezes considerados desnecessários pelos alunos. Ao vincular conceitos matemáticos a problemas de segurança da informação e ao uso de tecnologias, essa abordagem estimula a curiosidade e o envolvimento dos alunos, promovendo um aprendizado mais significativo e motivador.

3.2 Conceitos e Ferramentas Matemáticas

Nesta seção, abordamos os conteúdos matemáticos utilizados nas propostas de atividades da apostila, versando, sempre que necessário, sobre seus fundamentos, propriedades e demonstrações. Para tanto, utilizamos as referências (HEFEZ, 2016; SANTOS, 2000 e HYGINO, 2003) para a Subseção 3.2.1, (LIMA, 2013) para a Subseção 3.2.2, (BOLDRINI *et al.*, 1986 e HEFEZ, 2016) para a Subseção 3.2.3, (MORGADO, 2006; MORGADO, 2015) na Subseção 3.2.4 e (CASTANHEIRA, 2008) na Subseção 3.2.5.

3.2.1 Divisibilidade e divisão euclidiana

Como, no conjunto dos inteiros, a divisão de um número por outro nem sempre é possível, expressamos essa possibilidade por meio da relação de divisibilidade. Assim, quando não existir uma relação de divisibilidade entre dois números inteiros, ainda será possível efetuar uma “divisão com resto pequeno”, chamada de divisão euclidiana.

Definição 1: *Dados dois números inteiros* a *e* b*, diremos que* b *divide* a*, escrevendo* $b|a$*, quando existe um* $c \in Z$*, tal que* $a = cb$*. Neste caso, diremos que* b *também é um divisor ou um fator de* a *ou, ainda, que* a *é um múltiplo de* b *ou que* a *é divisível por* b*.*

É importante observar que, a notação $b|a$ não representa nenhuma operação em Z, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe um inteiro c, tal que, $a = cb$. A negação dessa sentença é representada por $b \nmid a$, significando que não existe nenhum número inteiro c, tal que, $a = cb$.

Por exemplo, $\pm 2|0$ pois existe um número inteiro $c = 0$, tal que, $0 = c.(\pm 2)$. Por outro lado, $0 \nmid (\pm 6)$, pois não existe um número inteiro c de tal forma que $(\pm 6) = c.0$.

Há infinitos casos de pares de inteiros tais que nenhum dos dois é divisor do outro. Por exemplo, 5 não é divisor de 3, nem 3 é divisor de 5. Assim, o algoritmo euclidiano que apresentaremos aqui, estabelece uma “divisão com resto” e é a base da aritmética teórica (Teoria dos Números). O nome do algoritmo euclidiano deriva do fato de Euclides o haver usado em seus Elementos 300 a.C. para determinar o máximo divisor comum de dois números positivos. A seguir, enunciamos o chamado Teorema de Eudoxius que é comumente conhecido como “Princípio de Arquimedes” (SANTOS, 2000) e, em seguida, enunciamos e demonstramos o Teorema do Algoritmo da Divisão, sendo este, um resultado central da Teoria dos Números.

Teorema 1: (*Teorema de Eudoxius) Dados* a *e* b *inteiros,* $b \neq 0$*, então:*
(i) a *é um múltiplo de* b *e, portanto* $a = qb$ *para algum* $q \in Z$*.*
(ii) a *está situado entre dois múltiplos consecutivos de* b*, isto é, existe* $q \in Z$ *tal que:*

- $qb \leq a < (q + 1)b; b > 0;$
- $qb \leq a < (q - 1)b; b < 0.$

Por exemplo, se $a = 11$ e $b = 4$, temos que $qb \leq a < (q + 1)b \Longrightarrow 2.4 \leq 11 < (2 + 1).4$. Da mesma maneira, podemos fazer a verificação da segunda desigualdade do Teorema considerando $b < 0$.

Teorema 2: *Sejam a e b dois números inteiros com $b > 0$, existe um único par de inteiros q e r tais que $a = qb + r$, com $0 \leq r < b$ (q é chamado de quociente e r de resto da divisão de a por b. Além disso, $r = 0 \Leftrightarrow b|a$).*

Demonstração:

a) Prova da existência de q e r:

Seja b um número inteiro estritamente positivo. Tomando-se algum inteiro a, temos duas possibilidades, ou seja, se $r = 0$, então a é um múltiplo de b e, portanto, $a = qb$ para um conveniente inteiro q, ou ainda, se $r \neq 0$, Pelo Teorema de Eudoxius, temos que a está situado entre dois múltiplos consecutivos de b. Como $b > 0$, então teremos $qb \leq a < (q + 1)b$. Somando-se $-qb$ em todos os termos da desigualdade, resulta em $0 \leq a - qb < b$. Fazendo $r = a - qb$, garantimos a existência de q e r na divisão de a por b pois, $r = a - qb \Longrightarrow a = qb + r; 0 \leq r < b$.

b) Prova da unicidade de q e r:

Sejam

$$a = q_1 b + r_1; 0 \leq r_1 < b \qquad (1)$$

$$a = q_2 b + r_2; 0 \leq r_2 < b. \qquad (2)$$

Suponha (por absurdo) que $q_1 \neq q_2$ e $r_1 \neq r_2$. De $r_1 \neq r_2$, temos que $r_1 > r_2$ ou $r_1 < r_2$. Suponha sem perda de generalidade, que $r_1 > r_2$. Igualando (1) e (2) obtemos:

$$q_1 b + r_1 = q_2 b + r_2 \Longrightarrow r_1 - r_2 = \left(q_2 - q_1\right)b.$$

Como $r_1 > r_2$, $r_1 - r_2 > 0$, logo, $q_2 - q_1 > 0$ e, dessa forma,

$$q_2 - q_1 \geq 1 \quad \Longrightarrow \quad (q_2 - q_1)b \geq b$$

$$\Longrightarrow \quad r_1 - r_2 \geq b$$

$$\Longrightarrow \quad r_1 \geq b + r_2,$$

o que é um absurdo pois $r_1 < b$. Portanto, $r_1 = r_2$ e consequentemente, $q_1 = q_2$.

Exemplo 1: Na divisão de 326 por $b > 0$, o quociente é 14 e o resto é r. Ache os possíveis valores de b e r.

Solução: Pelo Teorema de Eudoxius, como $b > 0$ temos que $14b \leq 326 < 15b$. Resolvendo essa desigualdade simultânea, obtemos $22 < b \leq 23$. Assim, temos duas possibilidades que satisfazem o problema, ou seja, $b = 22$ e $r = 18$ ou $b = 23$ e $r = 4$.

3.2.2 Funções

Sejam X e Y dois conjuntos quaisquer. Uma função é uma relação $f: X \longrightarrow Y$ que, a cada elemento $x \in X$, associa um, e somente um, elemento $y \in Y$. Além disso,

(i) Os conjuntos X e Y são chamados domínio e contradomínio de f, respectivamente;

(ii) O conjunto $f(X) = \{y \in Y; \exists\, x \in X,\ f(x) = y\} \subset Y$ é chamado imagem de f;

(iii) Dado $x \in X$, o (único) elemento $y = f(x) \in Y$ correspondente é chamado imagem de x.

Como estabelecido acima, uma função é um terno constituído pelos seguintes elementos: domínio, contradomínio e lei de associação (segundo a qual os elementos do domínio estão associados aos do contradomínio). Para que uma função esteja bem definida, é necessário que esses três componentes sejam dados. Observe que o enunciado dessa definição pode ser reescrito equivalentemente da seguinte forma: para que uma relação $f: X \longrightarrow Y$ seja uma função, esta deve satisfazer a duas condições fundamentais:

(I) estar definida em todo elemento do domínio (condição de existência);
(II) não fazer corresponder mais de um elemento do contradomínio a cada elemento do domínio (condição de unicidade).

Em diversas situações é interessante e até necessário definir a chamada função inversa de uma função dada. Como uma relação é qualquer forma de associar elementos de um conjunto X com elementos de um conjunto Y (ou qualquer subconjunto do produto cartesiano do conjunto X pelo conjunto Y, denotado por $X\times Y$), podemos sempre considerar a relação inversa de uma relação dada. Então, como definimos função como um tipo especial de relação, podemos sempre considerar a relação inversa de uma função (seja esta invertível como função ou não). Assim, determinar se uma função $f: X\longrightarrow Y$ tem ou não uma função inversa consiste em verificar se sua relação inversa é ou não uma função. Para isto, devemos verificar se essa relação inversa satisfaz as condições (I) e (II) anteriores. Para tanto, definimos três propriedades das funções em geral. Considere uma função $f: X\longrightarrow Y$. Então,
(1) f é sobrejetiva se para todo $y \in Y$, existe $x \in X$ tal que $f(x) = y$;
(2) *f* é injetiva se para $x_1, x_2 \in X$, $x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2)$;
(3) *f* é bijetiva se é sobrejetiva e injetiva.

Dessa forma, se a função original f é sobrejetiva, então f cobre todo o seu contradomínio, que é o domínio de sua relação inversa. Logo, sua relação inversa satisfaz a condição (I). Se f é injetiva, então cada $y \in Y$ está associado a um único $x \in X$. Então, a relação inversa satisfaz a condição (II). Decorre daí, que a relação inversa de f é uma função (isto é, que f tem uma função inversa) se, e somente se, f for sobrejetiva e injetiva, ou seja, se f for bijetiva.

O conceito de função está fortemente relacionado com uma das noções mais primordiais de toda a Matemática: a contagem. Na pré-história, mesmo antes de serem conhecidos os números ou a escrita, o homem já empregava processos de contagem. Esses processos consistiam basicamente em controlar uma quantidade por meio da comparação com objetos de referência, que em geral eram pequenas pedras ou marcações na rocha, na madeira ou em outros materiais. Em termos modernos, isto corresponde a estabelecer uma correspondência um a um, (o que chamamos de bijeção) entre dois conjuntos,

o que fazemos atualmente usando o conjunto dos números naturais (ou mais precisamente um de seus subconjuntos) como referência.

Assim, intuitivamente, podemos perceber que dois conjuntos têm o mesmo número de elementos se, e somente se, existe uma bijeção entre eles, o que é o mesmo que existir uma bijeção entre cada um deles e um mesmo subconjunto dos naturais. De fato, a ideia de bijeção é usada para enunciar a própria definição matemática de cardinalidade (ou número de elementos) de um conjunto. Dois conjuntos X e Y são ditos cardinalmente equivalentes (ou equipotentes) se existe uma bijeção $f: X \longrightarrow Y$.

Também, podemos relacionar a existência de funções injetivas e sobrejetivas com relações entre cardinalidades de conjuntos. Assim,

- Se existe uma injeção $f: X \longrightarrow Y$, então existe uma bijeção entre X e um subconjunto $Y' \subset Y$, isto é, X é cardinalmente equivalente a um subconjunto de Y.
- Se existe uma sobrejeção $f: X \longrightarrow Y$, então existe uma bijeção entre Y e um subconjunto $X' \subset X$, isto é, Y é cardinalmente equivalente a um subconjunto de X.

3.2.3 Matrizes

Dados $m, n \in N$, definimos uma matriz real de ordem m por n, ou simplesmente uma matriz m por n (denota-se $m \times n$), como uma tabela formada por números reais distribuídos em m linhas e n colunas. Os elementos que pertencem a uma matriz arbitrária são chamados de entradas da matriz. Um exemplo é a matriz 2×3 dada por

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

Onde as entradas da primeira linha da matriz são os números reais $2,\ 1,\ 0$ e as entradas da segunda linha são os números reais $-\ 1,\ -\ 2,\ 4$.

Para o caso de uma matriz genérica A, é comum indicarmos as entradas pelo símbolo a_{ij}, onde os índices ij indicam, respectivamente, a linha e a coluna onde o elemento se encontra. Dessa forma, representamos uma matriz genérica $m \times n$ por

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

Também podemos representar esta mesma matriz por $A = \left(a_{ij}\right)_{m\times n}$, ou ainda, apenas por $A = (a_{ij})$, quando a ordem estiver subentendida.

Algumas matrizes recebem nomes especiais de acordo com alguma característica que as mesmas possuam. Toda matriz $1\times n$ é chamada de *matriz linha,* e toda matriz $m\times 1$ é chamada de *matriz coluna*. Uma matriz $n\times n$ é chamada de *matriz quadrada de ordem* n. Por exemplo, a matriz

$$\begin{bmatrix} 1 & -3 & 1 & 0 & 4 \end{bmatrix}$$

é uma matriz linha de ordem 1×5 e a matriz

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

é uma matriz quadrada de ordem 3. Se $A = (a_{ij})$ é uma matriz quadrada de ordem n, as entradas a_{ij}, com $i = j$, formam a *diagonal principal* de A.

Uma *matriz diagonal de ordem* n é uma matriz quadrada de ordem n em que os elementos que não pertencem à diagonal principal são iguais a zero, ou seja, é uma matriz do tipo

$$\begin{bmatrix} a_{11} & \cdots & & 0 \\ \vdots & \ddots & & \vdots \\ & & \ddots & \\ 0 & \cdots & & a_{mn} \end{bmatrix}$$

A matriz diagonal de ordem n cujas entradas da diagonal principal são iguais a 1, dada por

$$\begin{bmatrix} 1 & \cdots & & 0 \\ \vdots & \ddots & & \vdots \\ & & \ddots & \\ 0 & \cdots & & 1 \end{bmatrix}$$

é chamada *matriz identidade de ordem* n e denotada usualmente por I_n.

Uma matriz $m\times n$ cujas entradas são todas iguais a zero é chamada *matriz nula*. Por exemplo, a matriz

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

é uma matriz nula de ordem 2×3.

Dizemos que duas matrizes $A = \left(a_{ij}\right)_{m\times n}$ e $B = \left(b_{ij}\right)_{m\times n}$, de mesma ordem, são *iguais*, escrevendo $A = B$, quando $a_{ij} = b_{ij}$ para todo $1\leq i\leq m$ e para todo $1\leq j\leq n$. Por exemplo, se x e y denotam números reais, temos que as matrizes

$$\begin{bmatrix} x & 0 \\ 1 & y \end{bmatrix} \text{ e } \begin{bmatrix} -1 & 0 \\ 1 & 2 \end{bmatrix}$$

são iguais quando $x = -1$ e $y = 2$.

O conjunto das matrizes $m\times n$ é munido de certas operações, algumas das quais definiremos a seguir:

(i) Soma: se $A = (a_{ij})$ e $B = (b_{ij})$ são duas matrizes de mesma ordem $m\times n$, a soma de A e B, denotada $A + B$, é a matriz $C = (c_{ij})$ de ordem $m\times n$ tal que $c_{ij} = a_{ij} + b_{ij}$, para todo $1\leq i\leq m$ e para todo $1\leq j\leq n$. Por exemplo

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

(ii) Subtração: dada uma matriz $A = (a_{ij})$, define-se a matriz oposta de A, como a matriz $-A = (-a_{ij})$. Por exemplo,

$$A = \begin{bmatrix} 5 & -3 \\ 1 & 8 \end{bmatrix} \text{ e } -A = \begin{bmatrix} -5 & 3 \\ -1 & -8 \end{bmatrix}$$

Tendo definido a operação de adição de matrizes e o conceito de matriz oposta, definimos a operação de *subtração* da maneira usual: dadas as matrizes A e B, então $A - B = A + (-B)$.

Dada a matriz $A = \left(a_{ij}\right)_{m\times n}$, definimos *o produto de A pelo número real a* (processo chamado de *multiplicação por escalar*), como sendo a matriz $aA = \left(a.a_{ij}\right)_{m\times n}$.Por exemplo,

$$-3 \cdot \begin{bmatrix} 2 & 0 \\ 1 & 1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -6 & 0 \\ -3 & -3 \\ 0 & 3 \end{bmatrix}$$

As operações de adição de matrizes e multiplicação por escalar descritas acima, conferem ao conjunto das matrizes $m\times n$ a estrutura de um espaço vetorial, para além destas, tal conjunto é ainda munido da operação de *multiplicação de matrizes*, definida a seguir.

Sejam $A = \left(a_{ij}\right)_{m\times n}$ e $B = \left(b_{ij}\right)_{n\times p}$, duas matrizes. O *produto* AB de A por B, denotado por AB, é definido como a matriz $C = \left(c_{ij}\right)_{m\times p}$, tal que,

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = a_{i1}b_{1j} + \ldots + a_{in}b_{nj} \tag{3}$$

para todo $1\leq i\leq m$ e para todo $1\leq j\leq p$. Por exemplo

$$\begin{bmatrix} 2 & 4 \\ 0 & 0 \\ -1 & 3 \end{bmatrix}\cdot\begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 2(-1)+4(1) & 2(1)+4(-1) \\ 0(-1)+0(1) & 0(1)+0(-1) \\ -1(-1)+3(1) & -1(1)+3(-1) \end{bmatrix} = \begin{bmatrix} 2 & -2 \\ 0 & 0 \\ -1 & -4 \end{bmatrix}$$

Note que, para o produto de A por B estar definido, o número de colunas de A deve ser igual ao número de linhas de B. Assim, se A e B são matrizes 2×3 e 3×1, respectivamente, o produto AB está definido e é uma matriz 2×1. Porém, o produto BA não está definido.

Uma condição necessária para que $AB = BA$ é que A e B sejam matrizes quadradas de mesma ordem. Contudo, esta condição não é suficiente. Por exemplo, as matrizes

$$A = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \text{ e } B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

são matrizes quadradas de ordem 2, mas $AB\neq BA$. Assim, vemos que a multiplicação de matrizes não possui a propriedade comutativa. Observe também que

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

sem que nenhuma das duas matrizes seja nula. Portanto, na multiplicação de matrizes, podemos ter $AB = 0$ sem que necessariamente A ou B sejam nulas. Lembremos que isto não ocorre com a multiplicação de números reais, pois dados dois números reais x e y tais que $xy = 0$, tem-se obrigatoriamente que $x = 0$ ou $y = 0$.

Tendo definido a multiplicação de matrizes, podemos definir os conceitos análogos aos de elemento neutro da multiplicação e inverso multiplicativo dos números reais para o conjunto das matrizes $m\times n$.

Uma consequência do modo como a multiplicação de matrizes é definida é que a multiplicação de uma matriz $m\times n$ por uma matriz identidade de ordem

n tem como resultado a própria matriz $m \times n$ original, ou seja $A.I_n = A$. Por exemplo

$$\begin{bmatrix} 2 & -1 \\ 5 & 7 \\ 0 & -4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 \cdot 1 + (-1) \cdot 0 & 2 \cdot 0 + (-1) \cdot 1 \\ 5 \cdot 1 + 7 \cdot 0 & 5 \cdot 0 + 7 \cdot 1 \\ 0 \cdot 1 + (-4) \cdot 0 & 0 \cdot 0 + (-4) \cdot 1 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 5 & 7 \\ 0 & -4 \end{bmatrix}$$

Genericamente:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

Dessa forma, a matriz identidade assume o papel de elemento neutro na operação de multiplicação matricial.

Dada uma matriz quadrada A de ordem n, chamamos de *inversa* de A a uma matriz quadrada B de ordem n, tal que, $AB = BA = I_n$. Por exemplo, dada a matriz

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

temos que a matriz

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

é uma inversa de A, já que $AB = BA = I_2$. Dessa forma, a matriz inversa assume o papel de inverso multiplicativo de uma matriz na operação de multiplicação matricial.

Note que uma matriz quadrada não possui necessariamente uma inversa. Por exemplo, seja a matriz nula de ordem 2

$$A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

temos que, para qualquer matriz genérica de ordem 2

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

resulta que

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \neq I_2$$

e, portanto, A não possui inversa.

Mesmo que uma matriz não seja nula, ela pode não ter inversa. Por exemplo, a matriz

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

não possui inversa, já que não existe uma matriz quadrada B de ordem 2 tal que $AB = I_2$.

Uma matriz quadrada A é dita *invertível* se A admite inversa. Se uma matriz A possui uma inversa, então essa inversa é única. Escrevemos A^{-1} para denotar a inversa de A.

3.2.4 Análise Combinatória

Análise Combinatória, ou simplesmente, Combinatória, é a parte da Matemática que analisa estruturas e relações discretas, lidando, de um modo mais geral, com a contagem, arranjo e combinação de elementos dentro de conjuntos. Dois tipos de problemas que ocorrem frequentemente em Análise Combinatória são:

1) Demonstrar a existência de subconjuntos de elementos de um conjunto finito dado e que satisfazem certas condições.

2) Contar ou classificar os subconjuntos de um conjunto finito e que satisfazem certas condições dadas.

Os principais conceitos abordados nessa disciplina incluem combinações, arranjos, permutações, e vários princípios fundamentais que são usados para resolver problemas de contagem sem a necessidade de listar todos os elementos do conjunto. Esses conceitos são fundamentais para diversos tópicos avançados, como a teoria de probabilidades. A seguir, apresentamos de maneira resumida, os principais conceitos e princípios fundamentais da Combinatória.

- **Princípio da Adição:** Se A e B são dois conjuntos disjuntos, isto é, que não possuem elementos em comum, com p e q elementos, respectivamente, então o número total de elementos na união desses conjuntos é dado por $p + q$. Este princípio é essencial para situações onde escolhas mutuamente exclusivas são feitas, permitindo a contagem de maneiras diferentes de ocorrer um ou outro evento.

- **Princípio da Multiplicação:** O princípio da Multiplicação, também chamado de *Princípio fundamental da contagem*, diz que se uma decisão d_1, pode ser tomada de x maneiras e, uma vez tomada d_1, uma decisão d_2 puder ser tomada de y maneiras, então o número total de maneiras de tomar as decisões d_1 e d_2 é xy. Este princípio é fundamental para contar o número de sequências de eventos onde cada evento depende do anterior.

- **Permutações:** Uma permutação é um arranjo (organização) ordenado de todos os elementos de um conjunto, o que pode ser entendido como um enfileiramento destes elementos. O número de permutações de n elementos é dado por $n!$ (fatorial de n), pois, em um total de n elementos, temos n modos de escolher um deles para ser o "primeiro da fila", após essa escolha restam $n-1$ elementos para enfileirar e portanto temos $n-1$ modos de escolher o "segundo da fila", analogamente, nossa terceira decisão pode ser tomada de $n-2$ modos e assim por diante; pelo princípio da multiplicação temos portanto $n(n-1)(n-2(n-3)...3.2.1 = n!$ modos de tomar as n decisões. Quando se considera permutações de n elementos onde alguns elementos são repetidos, é necessário ajustar a fórmula para evitar contar arranjos idênticos múltiplas vezes. Este conceito é amplamente aplicável em situações que envolvem a organização e ordenação de objetos.

- **Combinações:** Combinações referem-se à seleção de elementos de um conjunto onde a ordem em que são selecionados não importa, ou seja, duas ou mais seleções que acabem diferindo umas das outras apenas pela ordem de seus elementos contam como uma só. O número de combinações de n elementos tomados k de cada vez é dado por

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \qquad (4)$$

Para justificar esse resultado, basta observar que selecionar k objetos em um total de n objetos equivale a dividir os n objetos em um grupo de k objetos que são selecionados, e um grupo de $n - k$ objetos que são os não selecionados. Este conceito é crucial em situações onde o objetivo é selecionar grupos ou subconjuntos de um conjunto maior sem se importar com a ordem dos elementos selecionados.

- **Arranjos:** Arranjos referem-se à seleção de elementos de um conjunto onde a ordem importa. Ou seja, duas ou mais seleções que acabam diferindo umas das outras apenas pela ordem de seus elementos são consideradas como distintas. O número de arranjos de n elementos tomados k de cada vez é dado por

$$A(n,k) = \frac{n!}{(n-k)!} \tag{5}$$

Tal resultado se justifica pois para selecionar k objetos em um total de n , considerando distintas seleções dos mesmos objetos que diferem apenas pela ordem, podemos proceder como quem seleciona k pessoas de um total de n para formar uma fila, adaptando o raciocínio usado para as permutações para tal situação temos n modos de escolher o primeiro da fila, $n - 1$ modos de escolher o segundo, $n - 2$ modos de escolher o terceiro e assim por diante até a escolha do último que pode ser feita de $n - k + 1$ modos, logo, pelo princípio da multiplicação, temos um total de $n(n-1)(n-2)\ldots(n-k+1)$ modos de realizar tais escolhas, portanto temos:

$$n(n-1)\ldots(n-k+1) = \frac{n(n-1)(n-2)\ldots(n-k+1)(n-k)!}{(n-k)!} = \frac{n!}{(n-k)!} \tag{6}$$

Este conceito é essencial em situações onde a disposição dos elementos selecionados é relevante, como na organização de uma sequência específica de itens.

3.2.5 Estatística

A estatística é um conjunto de metodologias desenvolvidas para a coleta, classificação, apresentação, análise e interpretação de dados qualitativos e/ou quantitativos e a utilização desses dados como base para a tomada de decisões. Os métodos estatísticos são desenvolvidos para serem aplicados preferencialmente a um número alto de dados, visto que, através dos mesmos, procura-se encontrar tendências para o comportamento de conjuntos (chamados de população) de objetos ou seres e não para elementos em particular.

Um conjunto de dados ao qual aplicamos métodos estatísticos é obtido de um grupo de objetos de interesse chamado de amostra (BUSSAB, 2002). A amostra pode ser toda a população de interesse, ou apenas um subconjunto da mesma, sendo que, nesse segundo caso, existem metodologias específicas para a obtenção da amostra de acordo com a finalidade do estudo. Tais possibilidades para a amostra resultam em duas áreas específicas da estatística:

- **Estatística descritiva:** Trabalha com dados referentes a toda a população e portanto, temos ferramentas para procurar descrever melhor a população a partir desses dados.

- **Estatística inferencial:** Trabalha com dados de uma amostra da população que não equivale a sua totalidade, nesse caso os métodos descritivos são usados para entender a amostra e outros métodos são necessários para se elaborar inferências razoáveis sobre a população a partir da amostra.

Apresentamos a seguir, de maneira bastante resumida, alguns conceitos importantes em Estatística:

- **Variáveis qualitativas (ou categóricas):** Variáveis que representam categorias, ou seja, grupos de “valores” que se distinguem por características não numéricas.

- **Variáveis quantitativas (ou numéricas):** Variáveis que representam quantidades expressas em números. Podem ser discretas (contáveis) ou

contínuas (mensuráveis).

- **Frequência:** Número de vezes com que cada valor ou grupo de valores ocorre em um conjunto de dados. Pode representar também a frequência com que uma classe qualitativa ocorre na amostra. Quando expressa em números resultantes da contagem de vezes é chamada de frequência absoluta, quando expressa em porcentagem é chamada de frequência relativa.

- **Distribuição de frequências:** A distribuição de frequência é uma tabela que mostra as frequências das variáveis em uma amostra, podendo mostrar a frequência absoluta, relativa ou ambas em uma única tabela. A distribuição de frequências também pode ser expressa visualmente por meio de gráficos, quando é chamada de gráfico de frequência.

- **Medidas de tendência central:** São números que representam uma ideia dos valores mais típicos de uma variável em estudo. As principais são:

  (I) Média aritmética: O valor obtido pela razão entre a soma de todos os valores observados e o número de valores:

$$\bar{x} = \frac{x_1 + x_2 + \cdots + x_n}{n} \tag{7}$$

  II) Mediana: É definida como o valor com a propriedade de que metade dos valores são maiores ou iguais a este e a outra metade são menores ou iguais. Intuitivamente é o valor central quanto os valores são organizados em ordem crescente ou decrescente. Para o caso de um número par de valores definimos a mediana como a média aritmética dos dois valores centrais.

  III) Moda: É definida como o valor mais frequentemente observado de uma variável. Normalmente é de maior interesse para análise de variáveis qualitativas e variáveis numéricas discretas.

- **Medidas de dispersão:** São números que avaliam o quão espalhadas estão as observações de uma variável em torno de seus valores

centrais. As principais são:

I) Amplitude: É a mais simples das medidas de dispersão e indica apenas o quão distante estão um do outro os valores extremos observados. Assim, é definida como a diferença entre o maior valor e o menor.

II) Desvio padrão: É uma média adequada calculada sobre os desvios de cada observação em relação à média aritmética. Especificamente é calculado com a média quadrática dos desvios:

$$\sigma = \sqrt{\frac{(x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \cdots + (x_n - \bar{x})^2}{n}} \tag{8}$$

III) Coeficiente de variação: Resume as informações do desvio padrão em um valor adimensional (sem unidade de medida) através da divisão do desvio padrão pela média aritmética:

$$c_v = \frac{\sigma}{\bar{x}} \tag{9}$$

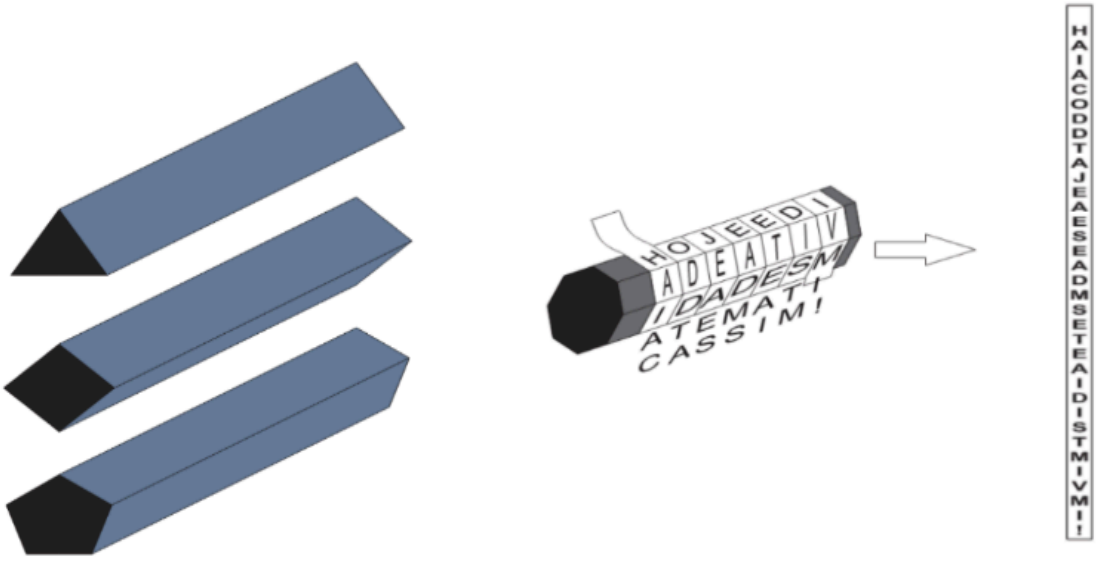
4. ATIVIDADES APLICADAS E SUAS EXPERIÊNCIAS NO ENSINO FUNDAMENTAL II E NO ENSINO MÉDIO

Este Capítulo apresenta o relato de uma aplicação prática de ferramentas de criptografia no ensino de Matemática para turmas do Ensino Fundamental II e do Ensino Médio. A criptografia, além de sua relevância contemporânea, serve como um excelente recurso didático para demonstrar a aplicação real da Matemática. As aulas envolveram a utilização de duas técnicas criptográficas: o citale e a criptografia por multiplicação de matrizes. No Ensino Fundamental II, os alunos decifraram mensagens utilizando a técnica do citale, enquanto no Ensino Médio, a atividade envolveu a cifragem e decifragem de mensagens por meio da multiplicação de matrizes.

4.1 O Citale

O citale é um prisma cuja base é um polígono regular, de modo que, ao redor de suas faces retangulares enrolamos uma tira de papel ou outro material para escrita e escrevemos uma mensagem ao longo do eixo longitudinal do citale conforme ilustrado na Figura 3.

Figura 3: Citales e o funcionamento da cifra do citale.



Fonte: o autor.

Quando desenrolamos a tira de papel, as letras ficam embaralhadas, obtendo-se assim a mensagem cifrada. Letras consecutivas do texto original se

encontrarão à uma mesma distância umas das outras no texto cifrado e, desta maneira, se enumerarmos as letras no texto cifrado de acordo com sua posição, a divisão do número relativo à posição pelo número de lados da base do citale deixará o mesmo resto quando as letras em questão forem consecutivas no texto original.

A atividade da cifra por citale foi aplicada em duas turmas de 9º ano do Ensino Fundamental II do Colégio Olímpio João Pissinati Guerra no Município de Sinop-MT. Nela, os alunos foram apresentados às noções básicas de criptografia e, posteriormente, separados em grupos, sendo desafiados a decifrar uma mensagem escrita em uma tira de papel.

Na sequência, foi apresentado pelo professor o método direto de decifragem onde as tiras foram enroladas nos citales adequados e a mensagem pôde ser lida.

Feito isso, cada grupo recebeu uma nova mensagem cifrada fornecida por outro grupo utilizando citales de papel cartão fornecidos pelo professor, cuja missão, consistiu em decifrá-la, sabendo que a cifragem usada foi a do citale, porém, sem usar o citale para decifrar e sem saber quantos lados tinha sua base. A intenção foi de que percebessem o padrão no posicionamento das letras nas tiras.

4.2 Multiplicação de Matrizes

Para criptografar uma mensagem através da multiplicação de matrizes usamos uma tabela predefinida para associar as letras a números. Dessa forma, podemos converter uma determinada mensagem em uma lista numérica, cujos números, podem ser usados como entradas de uma matriz.

Feito isso, multiplicamos a matriz obtida no passo anterior por uma outra chamada de chave, obtendo uma terceira matriz cujas entradas serão números que já não fazem sentido e que, por sua vez trata-se da mensagem cifrada.

Para que seja possível decifrar a mensagem, basta que a chave utilizada seja uma matriz invertível. Assim, multiplicamos a matriz produto pela inversa da chave, obtendo a matriz original, cujas entradas podem ser novamente convertidas em texto através da tabela usada no primeiro passo da cifragem.

Como ilustração do método, vamos cifrar e decifrar uma mensagem para descrever o passo a passo conforme ilustrado no Quadro 2.

Quadro 2: Descrição do método de cifragem e decifragem por meio de multiplicação de matrizes.

1º) Escolher uma mensagem para ser cifrada: em nosso caso escolhemos “BOM DIA”;

2º) Criar uma tabela e numerar as letras do alfabeto;

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

3º) Escrever os números correspondentes às letras da mensagem a ser cifrada;

B	**O**	**M**	**-**	**D**	**I**	**A**
2	15	13	27	4	9	1

4º) Criar a matriz chave que seja invertível (como os alunos deverão inverter a “Matriz Chave”, é interessante que a ordem seja 2, minimizando assim, a dificuldade dos alunos)

$$\text{Matriz Chave } = \begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix}$$

5º) Determinar a matriz que represente a mensagem que será cifrada (é importante atentar-se ao tamanho dessa matriz ao escolher o número de linhas e de colunas, pois esta matriz será multiplicada pela matriz chave);

$$\text{Matriz Mensagem } = \begin{bmatrix} 2 & 15 \\ 13 & 27 \\ 4 & 9 \\ 1 & 27 \end{bmatrix}$$

Obs: observe que seguimos a sequência dos números preenchendo a primeira coluna e em seguida a segunda coluna. Como a mensagem terminou antes de preenchermos todos os elementos da segunda coluna, inserimos no elemento a_{42} o número 27, que corresponde a um espaço.

6º) Para cifrar a mensagem “BOM DIA” basta multiplicar a “Matriz Mensagem” pela “Matriz Chave”;

7º) Para decifrar a mensagem por meio da matriz “Mensagem Cifrada”, basta multiplicar a matriz “Mensagem Cifrada” pela inversa da “Matriz Chave”;

$$\begin{bmatrix} 36 & 89 \\ 93 & 226 \\ 30 & 73 \\ 57 & 142 \end{bmatrix} \cdot \begin{bmatrix} 5 & -7 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 15 \\ 13 & 27 \\ 4 & 9 \\ 1 & 27 \end{bmatrix} = \text{Mensagem ”BOM DIA”}$$

$$\begin{bmatrix} 2 & 15 \\ 13 & 27 \\ 4 & 9 \\ 1 & 27 \end{bmatrix} \cdot \begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 36 & 89 \\ 93 & 226 \\ 30 & 73 \\ 57 & 142 \end{bmatrix} = \text{Mensagem Cifrada}$$

Fonte: o autor.

A atividade da cifra por operações matriciais foi aplicada em uma turma de 2º ano do Ensino Médio do Colégio Olímpio João Pissinati Guerra no Município de Sinop-MT. Inicialmente, os alunos foram apresentados ao conceito de matrizes e suas propriedades básicas, pois os mesmos ainda não haviam tido contato com esse conteúdo nas aulas de Matemática. Em seguida, foram definidas e exemplificadas a soma, a multiplicação por escalar e a multiplicação de matrizes. Após a introdução dos conceitos básicos, foi explicada e demonstrada a cifra por multiplicação de matrizes.

A atividade consistiu em cada grupo escolher uma frase, converter as letras em números através de uma tabela básica de associação alfanumérica e cifrar uma mensagem, multiplicando por uma matriz invertível.

Para a escolha da matriz invertível, algumas matrizes foram fornecidas pelo professor e cada grupo escolheu uma para usar como chave. Em seguida, as mensagens eram trocadas entre os grupos e cada grupo que recebia a mensagem de outro recebia também a chave (matriz) utilizada para cifrar, devendo, portanto, obter a inversa da chave, realizar a multiplicação conveniente e converter novamente os números obtidos em texto. As operações matriciais foram realizadas com o auxílio de uma calculadora online de matrizes (MATRIX CALCULATOR, 2023)[1].

4.3 Atividades propostas no 9º ano do Ensino Fundamental II

As atividades propostas foram trabalhadas em duas turmas do 9º ano do Ensino Fundamental II totalizando 47 participantes. Utilizamos 6 aulas correspondendo a 5 horas. Inicialmente, para que alcançar nossos objetivos, realizamos uma conversa introdutória com os alunos explicando de maneira simplificada o que é a criptografia e quais são os dois principais tipos de

[1] Ferramenta disponibilizada em https://matrixcalc.org/, o uso da mesma é bastante intuitivo havendo na interface células nas quais o usuário insere as entradas das matrizes, e botões referentes às diversas operações e cálculos que podem ser realizados (determinante, matriz inversa, produto de matrizes, escalonamento, etc).

técnicas de cifras de criptografia que seriam aplicadas (transposição e substituição), exemplificando tais técnicas por meio de diferentes exemplos e combinações possíveis para se realizar as cifras.

Propomos também, exercícios com mensagens cifradas para que os alunos pudessem decifrá-las, utilizando citales que foram construídos com papel cartão em momento anterior, sem tê-los apresentado aos alunos, para que pudessem colocar em prática sua criatividade e capacidade de resolução de um problema.

Nas duas últimas aulas, os alunos foram separados em grupos, em que cada grupo escolheu um citale e cifrou uma mensagem. Os grupos trocaram as mensagens entre si, de modo, que cada grupo sabia que a mensagem havia sido cifrada com citale, porém, não tinham acesso a esse citale e, dessa maneira, não sabiam quantas faces retangulares (lados) tinham os citales. O desafio era decifrar a mensagem.

Após a tentativa dos alunos, comentamos sobre a posição das letras em relação a mensagem original e as posições que estão sujeitas aos termos de uma Progressão Aritmética. Maiores detalhes em como esse método é utilizado está presente no produto educacional gerado por esta dissertação (ver Apêndice).

4.4 Atividades propostas no 2º ano do Ensino Médio

Para a turma do 2º ano do Ensino Médio, utilizamos 7 aulas em sala de aula, correspondendo a aproximadamente 6 horas para um total de 21 alunos.

Apresentamos para os alunos, um breve resumo do que é a criptografia e também um exemplo para cifrar e decifrar uma mensagem utilizando o citale. Como atividade, propomos a técnica de criptografia para cifrar mensagens utilizando a multiplicação de matrizes (um exemplo pode ser encontrado no Quadro 2).

Como os alunos não tinham estudado matrizes, foi necessário explicar os conceitos básicos de matrizes e operações de adição, multiplicação de um escalar por uma matriz e multiplicação entre matrizes, que seriam essenciais para aplicar as atividades. Utilizamos também a calculadora de matrizes *online* disponível em (MATRIX CALCULATOR, 2023), para realizarmos as

multiplicações entre matrizes e também a inversão de matriz devido ao pouco tempo para a realização da atividade.

Disponibilizamos uma tabela de associação das letras do alfabeto com números correspondentes aos alunos, também foram disponibilizadas matrizes de ordem 2 invertíveis para que os alunos pudessem escolher com matriz chave.

Feito isso, os alunos escolhiam uma mensagem para cifrar seguindo os passos do Quadro 2. Os alunos foram separados em grupos, de modo que, os grupos trocaram as mensagens entre si. O desafio consistiu em decifrar a mensagem.

4.5 Algumas reflexões e relatos sobre as atividades

A metodologia proposta em ambos os níveis de ensino incluiu aulas expositivas, demonstrações práticas pelo professor e atividades em grupo, onde os alunos aplicaram os conceitos aprendidos para resolver problemas de criptografia. Foram necessários momentos de revisão e preparação prévia dos conteúdos matemáticos pertinentes.

Em momento anterior à aplicação das atividades, elaboramos um questionário no modelo escala de Likert (MINDMINERS, 2023). Este modelo de questionário é interessante, visto que, por meio dele, podemos investigar e mensurar atitudes ou comportamentos dos alunos para direcionar novas estratégias para aplicações futuras.

Dessa maneira, após a execução das atividades tanto para o 9º ano do Ensino Fundamental II como para o 2º ano do Ensino Médio, aplicamos um questionário que nos ajudou a compreender os sentimentos de frustração e expectativa dos alunos. Isso é fundamental para entendermos como uma aplicação em sala de aula pode ser trabalhada e melhorada constantemente, buscando sempre, atender a um público de alunos específicos.

A aplicação dessas atividades em sala de aula revelou-se engajadora, possivelmente facilitando o aprendizado dos conceitos matemáticos. Os alunos demonstraram maior interesse e compreensão do conteúdo ao perceberem suas aplicações práticas.

No Capítulo 5, em nossas discussões, detalharemos como se deu a aplicação dos questionários, destacando e discutindo os principais resultados. De um modo geral, as avaliações realizadas por meio dos questionários, mostraram um considerável nível de satisfação e engajamento dos alunos, destacando a eficácia das atividades propostas.

Apresentamos a seguir, algumas observações sobre a aplicação das atividades:

- É importante salientar que alguns pontos da atividade devem ser feitos de modo a não gastar muito tempo, para que sobre tempo para a realização de outros pontos. Por exemplo, em nosso caso, os grupos demoraram muito para escolher a frase a ser cifrada sendo que essa deve ser uma etapa rápida da atividade.
- É ideal verificar junto aos grupos se a escrita na tira do citale foi feita corretamente para que eventuais erros não comprometam a decifragem. No caso da atividade com matrizes, os alunos devem se atentar à correta correspondência entre letras e números.
- No caso do citale, o ideal é que as mensagens sejam escritas em letras de fôrma, pois as letras ficarão separadas uma das outras e nessa configuração as letras cursivas podem causar confusão quanto a letra específica escrita. No caso das matrizes devem se atentar à legibilidade dos números escritos na mensagem que será passada à outro grupo.
- Os alunos parecem possuir uma predileção por soluções analógicas de problemas no lugar de soluções analíticas, no caso da cifragem por citale onde os grupos sabiam que um citale havia sido utilizado para cifrar a mensagem mas não sabiam qual, muitos alunos tentaram decifrar a mensagem enrolando a tira no braço, em garrafinhas ou coisas do tipo e alguns até montaram citales às pressas com folhas de caderno para tentar decifrar.
- Na cifragem por citale, a princípio muitos alunos não notaram que se escreverem as letras da mensagem cifrada em tabelas, a decifragem será imediata quando o número de linhas (ou colunas, dependendo de em qual direção eles distribuírem as letras) for igual ao número de faces retangulares do citale utilizado.

- Na atividade com matrizes, os grupos, em geral, entenderam bem rápido como se utilizar a calculadora de matrizes, tanto para multiplicação de matrizes como para encontrar a matriz inversa.
- Algumas dificuldades foram encontradas, entre elas: a preocupação dos alunos com a escolha da frase a ser cifrada, o que levou à uma demora na escolha da frase. Um outro ponto é a escrita de determinados alunos que muitas vezes não era compreendida por colegas de outro grupo. No caso do ensino fundamental, houve pouca cooperação em alguns grupos.
- Um questionário no modelo da escala de Likert (MINDMINERS, 2023) foi elaborado e aplicado aos alunos que participaram das atividades para que os mesmos avaliassem alguns aspectos da aula. O questionário focou em obter dados quanto a satisfação dos alunos com as atividades realizadas e a potencialidade das atividades como engajadora e facilitadora do ensino de Matemática.

5. DISCUSSÕES E CONCLUSÕES

Durante a execução de nossa pesquisa, tivemos a oportunidade de vivenciar o ensino e a aprendizagem de um ponto de vista diferente do ensino tradicional. Ao trabalharmos com algumas ferramentas de criptografia, observamos a motivação e a compreensão dos alunos durante todo o processo de aquisição de novos conhecimentos. Isso se mostrou notório nas respostas do questionário que foi aplicado após a execução das atividades tanto para o 9º ano do Ensino Fundamental II como para o 2º ano do Ensino Médio.

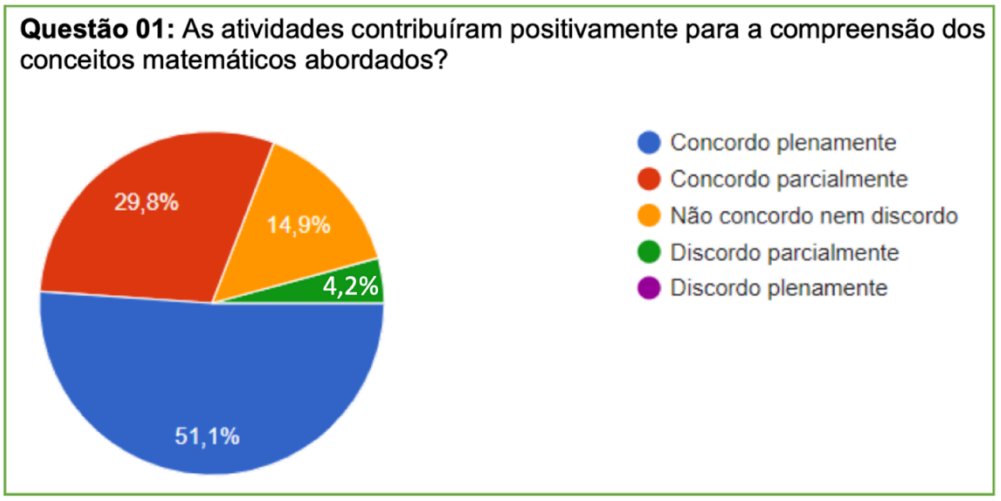
No Anexo I, apresentamos o questionário contendo 8 questões que foi aplicado ao 9º ano do Ensino Fundamental II e ao 2º ano do Ensino Médio. As perguntas e afirmações presentes no questionário são as mesmas em ambas as turmas por tratarem-se de questionamentos gerais podendo ser estendido para estudantes de diferentes faixas etárias.

Os questionários foram elaborados utilizando-se um formulário do Google, podendo este ser elaborado a partir de um ícone presente no Google apps de qualquer conta de e-mail da Google. O formulário contendo o questionário foi respondido pelos alunos utilizando-se os dispositivos Chromebooks disponíveis no colégio para uso pedagógico pelos mesmos.

5.1 Resultados e Análise do Questionário aplicado nas turmas do 9º ano do Ensino Fundamental II

Participaram da atividade proposta 47 alunos do 9º ano do Ensino Fundamental II. A primeira questão teve por objetivo identificar se as atividades contribuíram positivamente para a compreensão dos conceitos matemáticos abordados. De acordo com a Figura 4, 80,9% dos alunos consideraram que as atividades contribuíram totalmente ou parcialmente para sua compreensão e aprendizado dos conteúdos propostos. Apenas 4,2% dos alunos mostraram-se parcialmente insatisfeitos com a atividade e 14,9% não formaram nenhuma opinião sobre a atividade proposta.

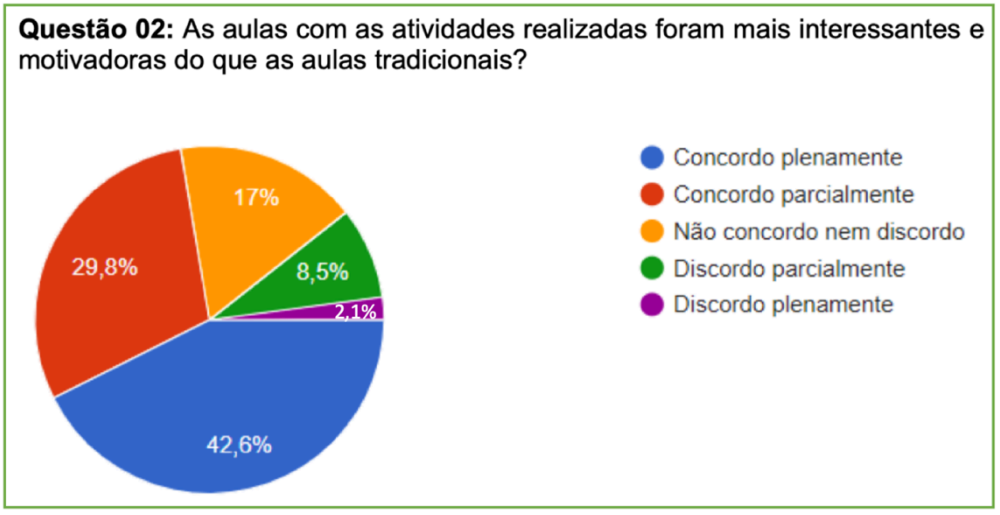
Figura 4 : Gráfico do percentual das respostas da questão 01 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

A segunda questão teve por objetivo identificar se as atividades foram mais interessantes e motivadoras do que as aulas tradicionais. De acordo com a Figura 5, 72,4% dos alunos consideraram que as atividades foram de algum modo motivadoras, porém 10,6% dos alunos se identificam mais com aulas no formato tradicional e 17% não formaram nenhum tipo de opinião a respeito. Isso mostra que, para esta turma em especial, mesclar atividades que envolvam práticas educacionais alternativas com o ensino tradicional é mais interessante.

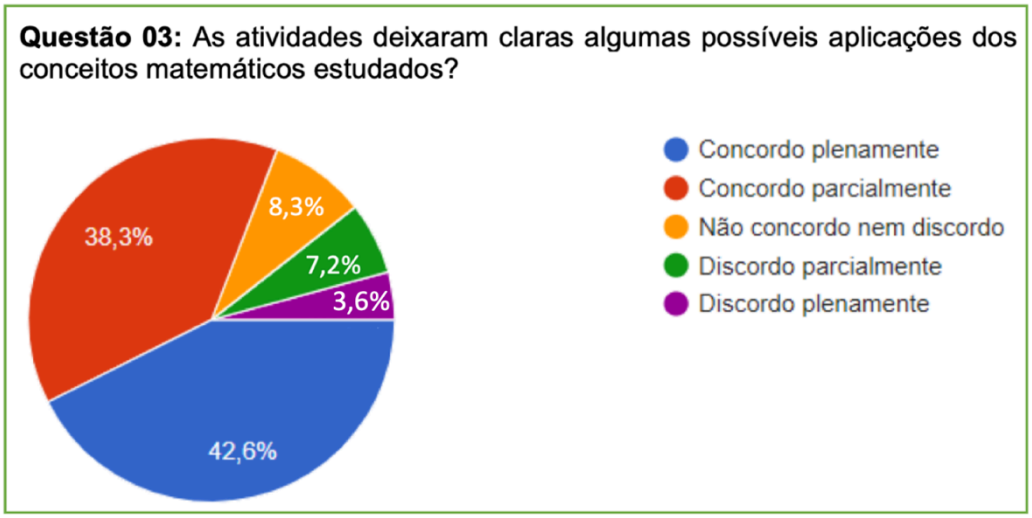
Figura 5: Gráfico do percentual das respostas da questão 02 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

A terceira questão buscou identificar se as atividades deixaram claras algumas possíveis aplicações dos conceitos matemáticos estudados. De acordo com a Figura 6, 80,9% dos alunos consideraram de um modo geral, que as atividades deixaram claras possíveis aplicações dos conceitos matemáticos estudados, porém 10,8% discordaram e 8,3% não formaram nenhuma opinião.

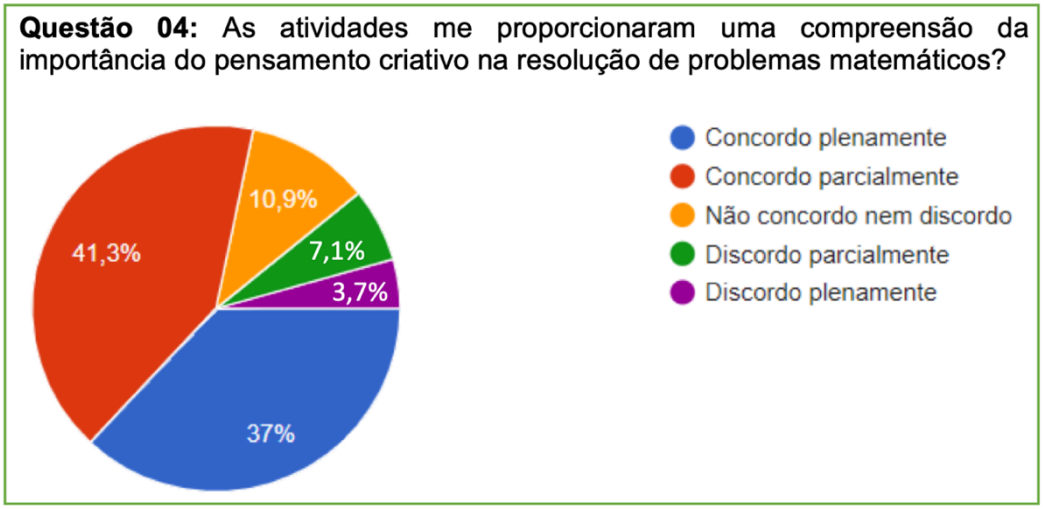
Figura 6: Gráfico do percentual das respostas da questão 03 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

Na quarta questão o objetivo consistiu em identificar se as atividades proporcionaram ao aluno a compreensão da importância do pensamento criativo na resolução de problemas matemáticos. De acordo com a Figura 7, 78,3% dos alunos concordaram positivamente, porém, 10,8% discordaram e 8,3% não formaram nenhuma opinião.

Figura 7: Gráfico do percentual das respostas da questão 04 do questionário.



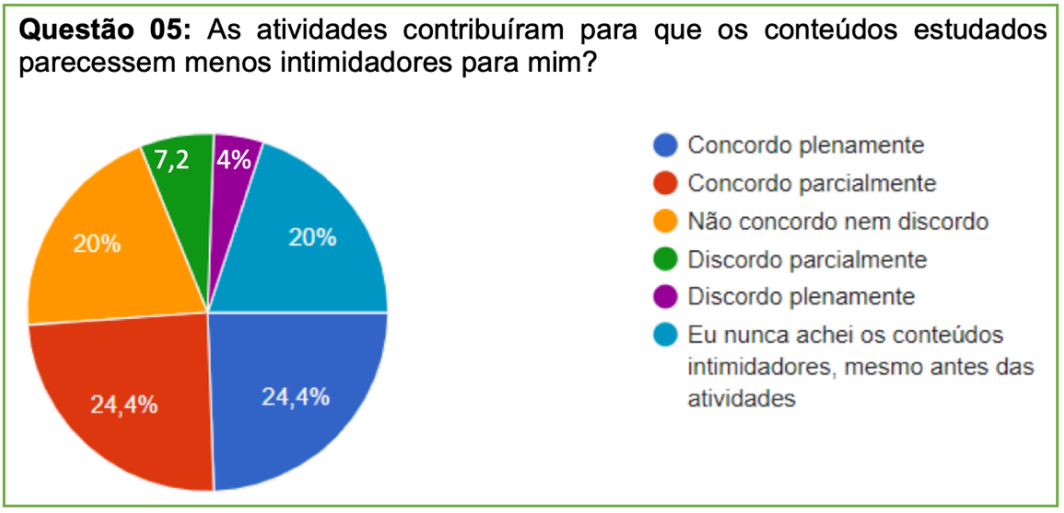
Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

Na quinta questão, cujo foco era investigar se as atividades contribuíram para que os conteúdos estudados parecessem menos intimidadores, o gráfico percentual das respostas, indicou que para 48,8% dos alunos as atividades contribuíram para tornar os conteúdos menos intimidadores.

Nessa pergunta, houve um aumento no percentual dos alunos que não formaram nenhuma opinião, ou seja, 20% dos alunos não conseguiram (ou não quiseram) identificar se as atividades fizeram ou não alguma diferença nesse quesito.

Apenas uma minoria de 4%, consideraram que as atividades não ajudaram para tornar o conteúdo menos intimidador e 20% dos alunos não apresentaram problemas quanto aos conteúdos, conforme ilustrado na Figura 8.

Figura 8: Gráfico do percentual das respostas da questão 05 do questionário.

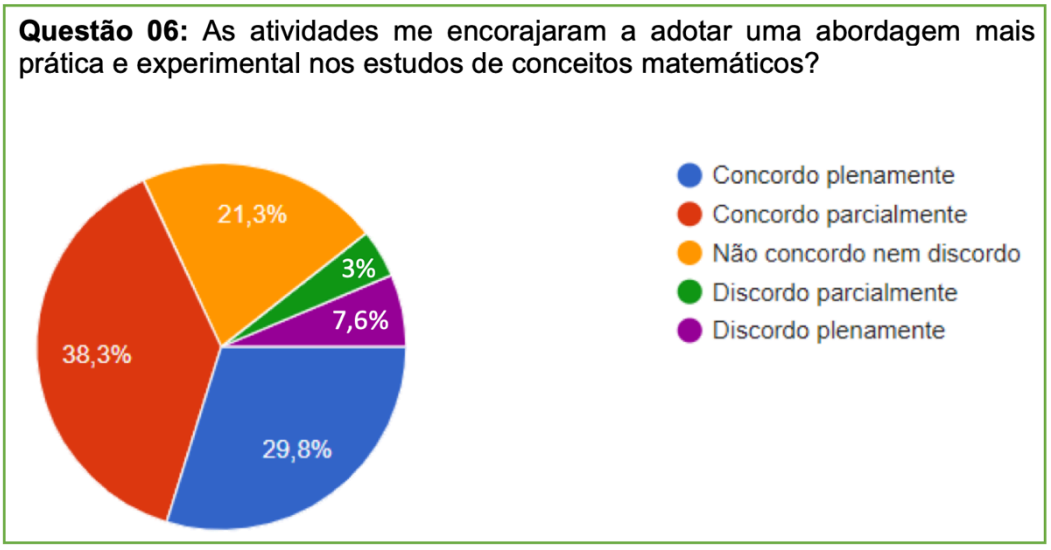


Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

A sexta questão buscou identificar se as atividades encorajaram os alunos a adotar uma abordagem mais prática e experimental nos estudos de conceitos matemáticos.

De acordo com a Figura 9, 68,1% dos alunos concordaram com a questão, 21,3% não assumiu nenhuma opinião, indicando que talvez não tenham compreendido a questão e, 10,6% indicaram que as atividades em nada contribuíram para esse quesito.

Figura 9: Gráfico do percentual das respostas da questão 06 do questionário.

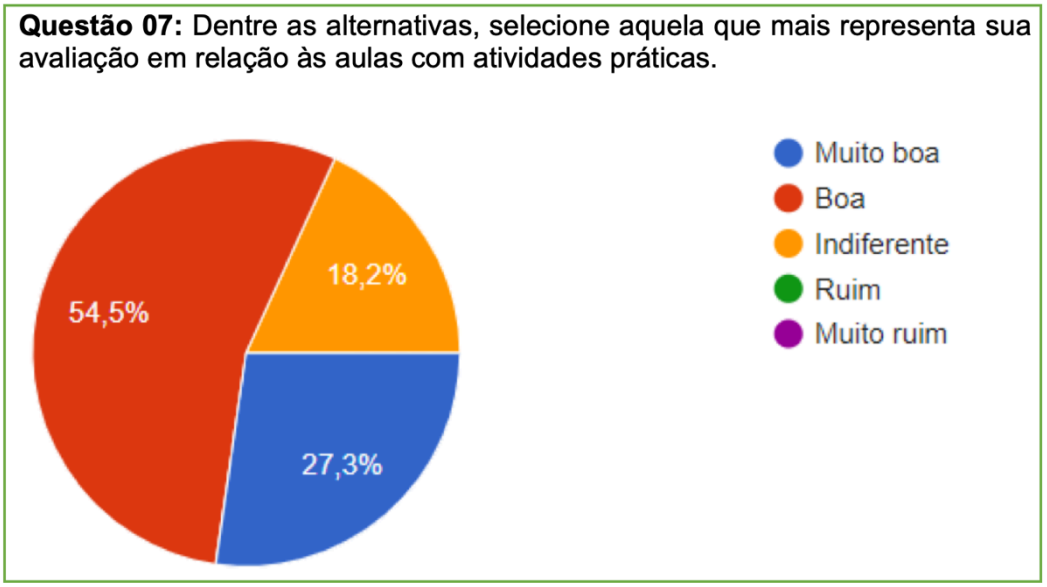


Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

A sétima questão teve por objetivo, avaliar as aulas com atividades práticas.

De acordo com a Figura 10, 81,8% dos alunos avaliaram as aulas como sendo boa ou muito boa, 18,2% não opinaram e não houveram indicativos negativos para as aulas com atividades práticas. Acreditamos que, em virtude do alto percentual de aceitação das aulas com atividades práticas, talvez os alunos não tenham conseguido se expressar corretamente em algumas das perguntas anteriores, visto que, as respostas dos alunos acabam tornando-se contraditórias.

Figura 10: Gráfico do percentual das respostas da questão 07 do questionário.

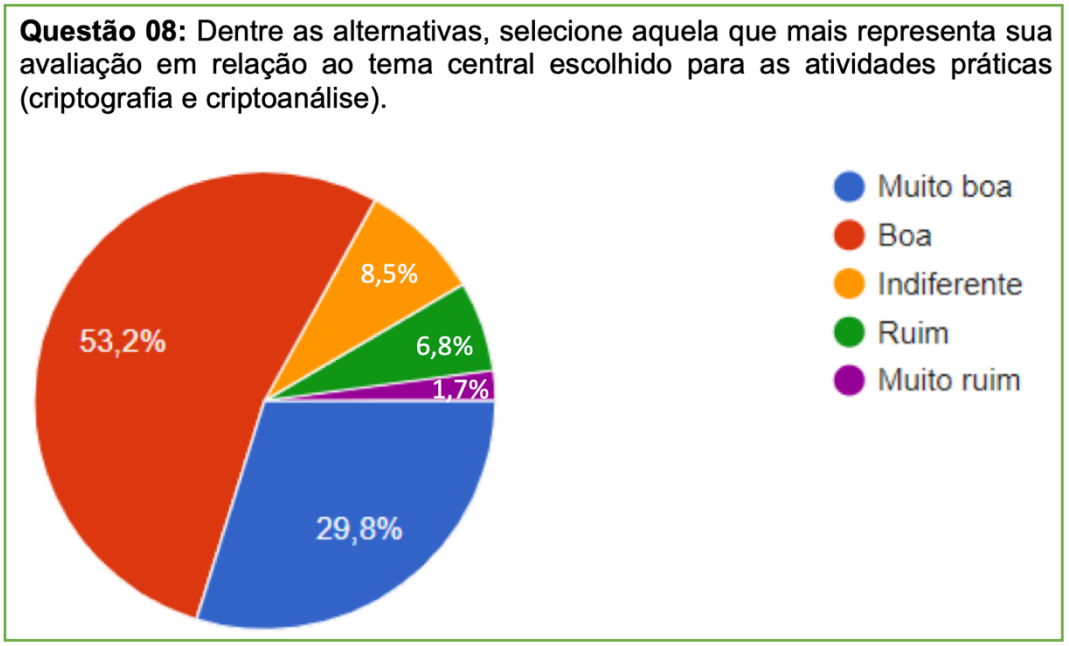


Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

Finalmente, a oitava e última questão, avaliou a relação entre o tema central escolhido para as atividades práticas.

De acordo com a Figura 11, a grande maioria dos alunos correspondendo a 83% julgaram que, o tema para as atividades, foram bom ou muito bom. Entretanto, 8,5% não opinaram e, 8,5% não gostaram do tema escolhido para as atividades práticas.

Figura 11: Gráfico do percentual das respostas da questão 08 do questionário.



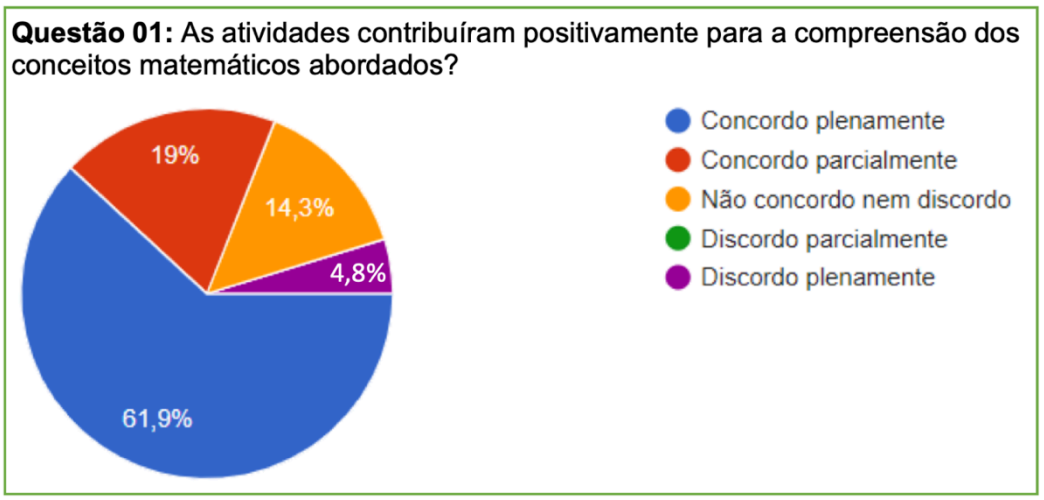
Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

5.2 Resultados e Análise do Questionário aplicado na turma do 2º ano do Ensino Médio

De maneira análoga, fizemos a mesma análise para a turma de alunos do 2º ano do Ensino Médio. Desta vez, apenas 21 alunos participaram da pesquisa.

De acordo com a Figura 12, 80,9% dos alunos consideraram que as atividades contribuíram totalmente ou parcialmente para sua compreensão e aprendizado dos conteúdos propostos. Apenas 4,8% dos alunos mostraram-se parcialmente insatisfeitos com a atividade e 14,3% não formaram nenhuma opinião sobre a atividade proposta.

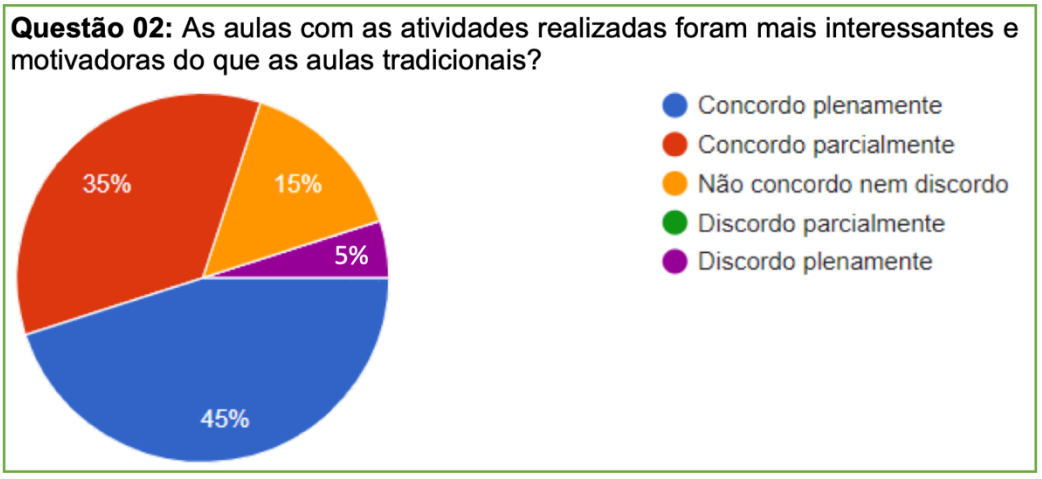
Figura 12: Gráfico do percentual das respostas da questão 01 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

A segunda questão teve por objetivo identificar se as atividades foram mais interessantes e motivadoras do que as aulas tradicionais. De acordo com a Figura 13, 80% dos alunos consideraram que as atividades foram de algum modo motivadoras, porém 5% dos alunos se identificam mais com aulas no formato tradicional e 15% não formaram nenhum tipo de opinião a respeito.

Figura 13: Gráfico do percentual das respostas da questão 02 do questionário.

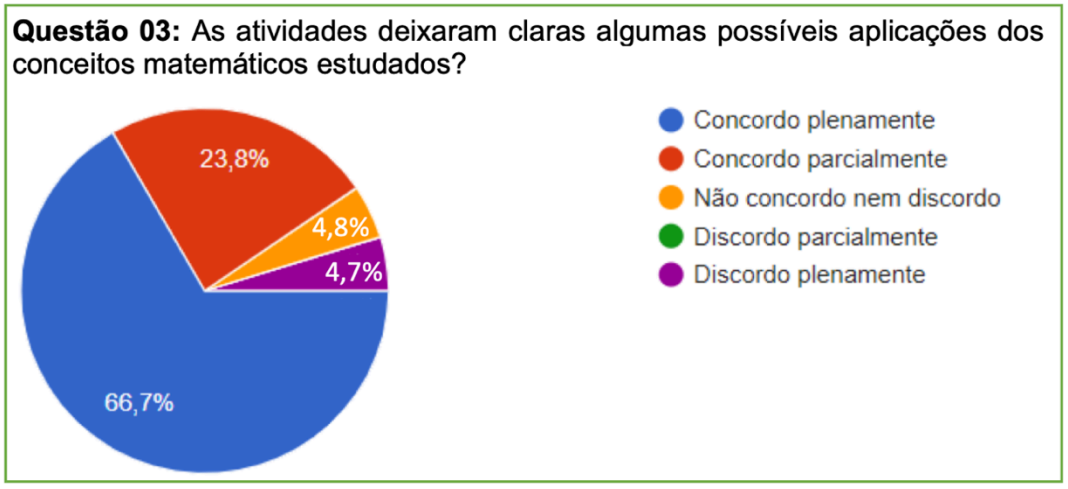


Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

A terceira questão buscou identificar se as atividades deixaram claras algumas possíveis aplicações dos conceitos matemáticos estudados. De acordo com a Figura 14, 90,5% dos alunos consideraram de um modo geral,

que as atividades deixaram claras possíveis aplicações dos conceitos matemáticos estudados, porém 4,7% discordaram e 4,8% não formaram nenhuma opinião.

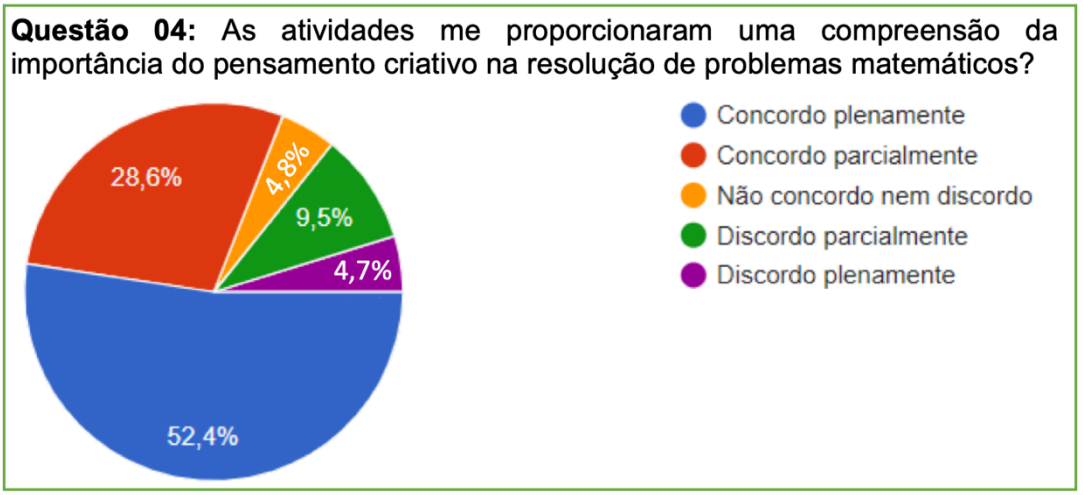
Figura 14: Gráfico do percentual das respostas da questão 03 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

Na quarta questão o objetivo consistiu em identificar se as atividades proporcionaram ao aluno a compreensão da importância do pensamento criativo na resolução de problemas matemáticos. De acordo com a Figura 15, 81% dos alunos concordaram positivamente, porém, porém 14,2% discordaram e 4,8% não formaram nenhuma opinião.

Figura 15: Gráfico do percentual das respostas da questão 04 do questionário.



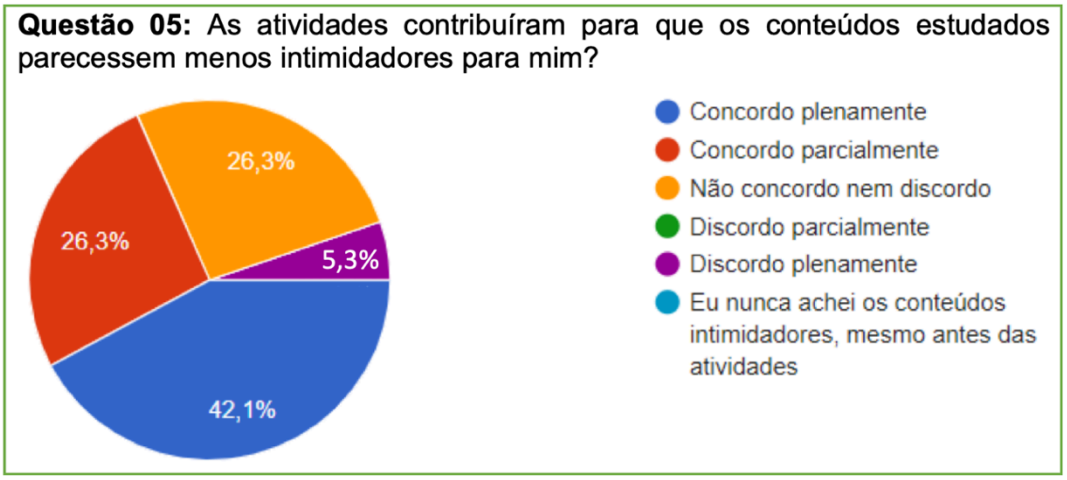
Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

Na quinta questão, cujo foco era investigar se as atividades contribuíram para que os conteúdos estudados parecessem menos intimidadores, o gráfico

percentual das respostas, indicou que para 68,4% dos alunos as atividades contribuíram para tornar os conteúdos menos intimidadores.

Apenas uma minoria de 5,3%, consideraram que as atividades não ajudaram para tornar o conteúdo menos intimidador e 26,3% dos alunos não emitiram nenhuma opinião, conforme ilustrado na Figura 16.

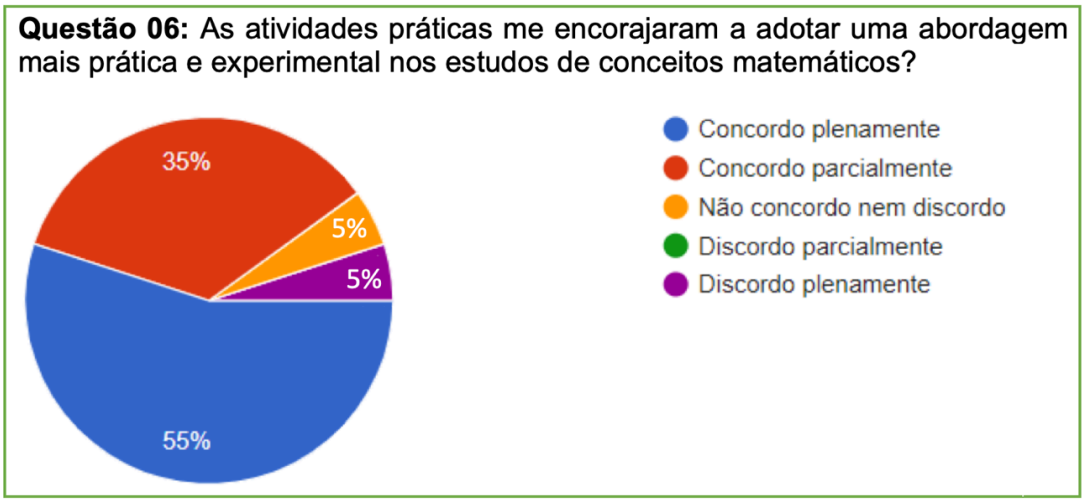
Figura 16: Gráfico do percentual das respostas da questão 05 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

A sexta questão buscou identificar se as atividades encorajaram os alunos a adotar uma abordagem mais prática e experimental nos estudos de conceitos matemáticos. De acordo com a Figura 17, 90% dos alunos concordaram com a questão, 5% não assumiu nenhuma opinião e 5% indicaram que as atividades em nada contribuíram para esse quesito.

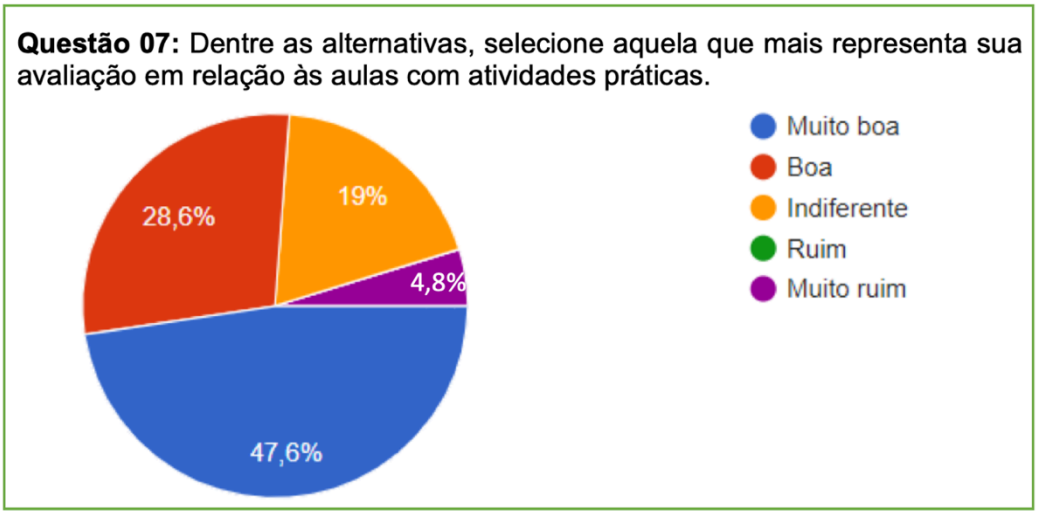
Figura 17: Gráfico do percentual das respostas da questão 06 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

A sétima questão teve por objetivo, avaliar as aulas com atividades práticas. De acordo com a Figura 18, 70,2% dos alunos avaliaram as aulas como sendo boa ou muito boa, 19% não opinaram e 4,8% acharam as atividades práticas muito ruins.

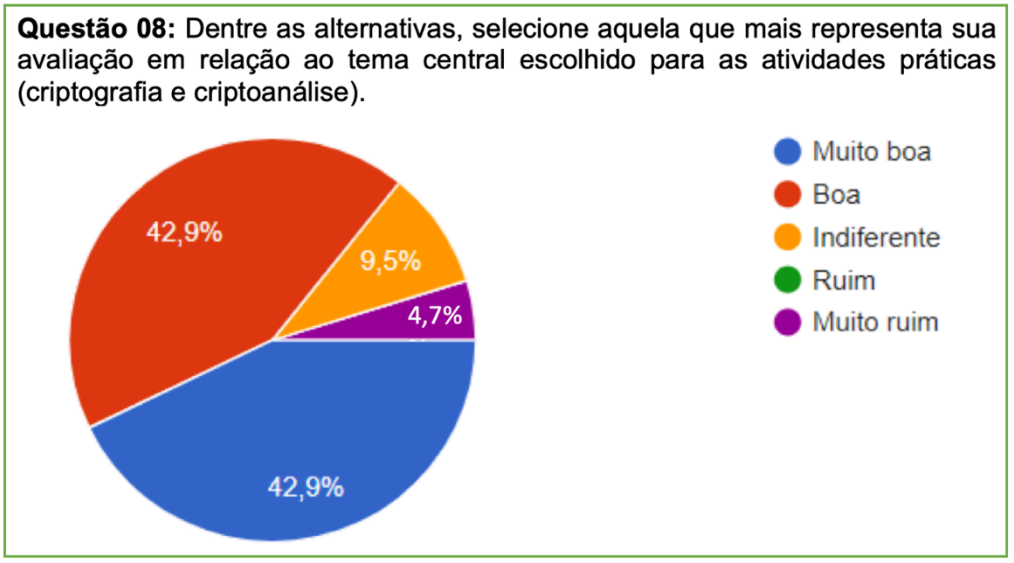
Figura 18: Gráfico do percentual das respostas da questão 07 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

Finalmente, a oitava e última questão, avaliou a relação entre o tema central escolhido para as atividades práticas. De acordo com a Figura 19, a grande maioria dos alunos correspondendo a 85,8% julgaram que, o tema para as atividades, foi bom ou muito bom. Entretanto, 9,5% não opinaram e, 4,7% não gostaram do tema escolhido para as atividades práticas.

Figura 19: Gráfico do percentual das respostas da questão 08 do questionário.



Fonte: o autor (gráfico gerado pelo formulário do Google de acordo com as respostas dos alunos).

5.3 Reflexões finais

Concluímos que, embora os conteúdos matemáticos trabalhados, bem como as atividades práticas elaboradas e executadas em turmas do Ensino Fundamental II e Ensino Médio sejam abordados em nível básico, é importante salientar que a maturidade dos alunos influencia fortemente nas respostas obtidas dos questionários. Como observado, das Seções 5.1 e 5.2, os alunos do Ensino Médio responderam o questionário indicando uma abertura maior à aplicação de atividades diversas em sala de aula para a aquisição de conhecimentos matemáticos. Um indicativo é que, por serem adolescentes, talvez tenham um contato maior com desafios do cotidiano e vinculados as tecnologias digitais. Assim, sentem-se mais confortáveis diante de desafios. Também devemos levar em consideração os alunos que se omitiram diante de um posicionamento favorável ou desfavorável. Vale investigar as razões pelas quais esses alunos não conseguiram se posicionar. E finalmente, temos os alunos que não gostaram das atividades. Mesmo sendo um percentual baixo, é dever do professor amparado pela instituição compreender a insatisfação desses alunos diante da aquisição de novos conhecimentos por alternativas diferentes das tradicionais.

Finalmente, podemos acrescentar que por meio dessa pesquisa foi possível gerar um produto educacional na forma de apostila contendo diferentes atividades envolvendo criptografia, cuja expectativa é que sirva de material de apoio para atividades diferenciadas a professores do Ensino Fundamental e Ensino Médio. A apostila está presente no Apêndice deste trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

AUSUBEL, D. P.. **A aprendizagem significativa: a teoria de David Ausubel**. São Paulo: Moraes, 1982.

AUSUBEL, D.P.. **Psicologia Educacional: Uma Visão Cognitiva.** Nova York, NY: Holt, Rinehart e Winston, 1968.

BALL, D. L.. **As compreensões matemáticas que os futuros professores trazem para a formação de professores**. - Reston, VA: Conselho Nacional de Professores de Matemática, 1990.

BLUMENFELD, P.C., SOLOWAY, E., MARX, R.W., KRAJCIK, J.S. GUZDIAL, M., & PALINCSAR, A.. **Motivando a aprendizagem baseada em projetos: Sustentando o fazer, apoiando a aprendizagem.** Psicólogo Educacional, 26(3-4), 369-398, 1991.

BOALER, J.. **Mentalidades matemáticas: liberando o potencial dos alunos por meio de matemática criativa, mensagens inspiradoras e ensino inovador.** - San Francisco, CA: Editora Jossey-Bass, 2016.

BOLDRINI, J. L. [et al.]. **Álgebra Linear** – 3ª. ed - São Paulo: Harbra, 1986.

BRASIL. **Ministério da Educação. Base Nacional Comum Curricular**. Brasília: MEC, 2017.

CASTANHEIRA, N.P.. **Estatística aplicada a todos os níveis**. 4. ed. rev. e atual. - Curitiba : Ibpex, 2008.

CASTELLAR, S.. **A construção do pensamento algébrico na escola: desafios e possibilidades.** Belo Horizonte: Autêntica Editora, 2014.

CHEFE, S.. **Aprendizagem baseada em projetos: ensino diferenciado para o século XXI.** Thousand Oaks, CA: Corwin Press, 2018.

D'AMBRÓSIO, U.. **Educação matemática: da teoria à prática.** Campinas: Papirus, 1996.

DEWEY, J.. **Democracia e Educação: introdução à filosofia da educação.** 4.ed. John Dewey ; tradução de Godofredo Rangel e Anísio Teixeira. — 4. ed. — São Paulo : Ed. Nacional, 1979.

DOMINGUES, H. H.. **A aprendizagem significativa: a teoria de David Ausubel**. São Paulo: Moraes, 1982.

FIORENTINI, D. e LORENZATO, S.. **Investigação em educação matemática: percursos teóricos e metodológicos.** Campinas: Autores Associados, 2006.

FREIRE, P.. **Pedagogia do Oprimido**. - Rio de Janeiro: Editora Paz e Terra, 1973.

HEFEZ, A.. **Aritmética.** Rio de Janeiro: SBM, 2016.

HEFEZ, A., FERNANDES, C. S.. **Introdução à Álgebra Linear**. Rio de Janeiro: SBM, 2016.

LIMA, E. L.. **Número e Funções Reais**. Rio de Janeiro: SBM, 2013.

LIMA, E.L., WAGNER, E., CARVALHO, P.C.P. MORGADO, A.C.. **Temas e Problemas Elementares**. 5.ed. -Rio de Janeiro: SBM, 2013.

MATRIX CALCULATOR. Disponível em: https://matrixcalc.org/pt/. Acesso em: 25/10/2023.

MELO, C. D. L. (2014). **Criptografia no Ensino Médio: uma Proposta para o Ensino de Matrizes**. Dissertação de Mestrado, Universidade Estadual de Campinas, Campinas.

MINDMINERS. Disponível em: https://mindminers.com/blog/entenda-o-que-e-escala-likert/. Acesso em: 05/04/2024.

MORGADO, A.C.O, CARVALHO, J.B.P., FERNANDEZ, P.C.P.. **Análise combinatória e probabilidade: com as soluções dos exercícios**. 9. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006.

MORGADO, A. C.O., CARVALHO, P.C.P.. **Matemática Discreta**. Rio de Janeiro: SBM, 2015.

OLIVEIRA, M.K.. **Vygotsky: aprendizagem e desenvolvimento de um processo sócio-histórico.** São Paulo: Cipione, 2016.

PEREIRA, N. M. I. (2015). **Criptografia: uma nova proposta de ensino de matemática no ciclo básico**. Dissertação de Mestrado, Universidade Estadual Paulista Júlio de Mesquita Filho, Instituto de Biociências, Letras e Ciências Exatas, Rio Claro, SP.

PONTES, E. A. S., SILVA, B. H. M. S., & OLIVEIRA, E. G. (2022). **Criptografia em Funções Polinomiais: Um Processo de Ensino e Aprendizagem de Matemática na Educação Básica**. The Journal of Engineering and Exact Sciences, 8(6), 14609-01e.

SANTOS, J.P.O.. **Introdução à Teoria dos Números.** Rio de Janeiro: IMPA, 2000.

SILVA, M. V., EVANGELISTA, D. H. R., & EVANGELISTA, C. J. (2022). **Tecnologias digitais aliadas ao ensino de Criptografia**. The Journal of Engineering and Exact Sciences, 8(5), 14313-01e.

SINGH, S.. **O Livro dos Códigos: A ciência do sigilo - do antigo Egito à criptografia quântica.** Tradução de Jorge Calife - 15ª ed. - Rio de Janeiro: Record, 2023.

THOMAS, J.W.. **Uma revisão da pesquisa sobre aprendizagem baseada em projetos.** San Rafael, CA: Fundação Autodesk, 2000.

VIDAL, S. C., CAPRI, M. R., & ROMÃO, E. C. (2022). **Cryptography as an Educational Tool in Counting Techniques for High School**. International Journal for Innovation Education and Research, 10(5), 76-88.

VYGOTSKY, L.S. **Mente na Sociedade: O Desenvolvimento de Processos Psicológicos Superiores.** Cambridge, MA: Harvard University Press, 1978.

APÊNDICE

APÊNDICE 1: APOSTILA DE PROPOSTAS DE ATIVIDADES

UNIVERSIDADE DO ESTADO DE MATO GROSSO
CAMPUS DE SINOP
FACULDADE DE CIÊNCIAS EXATAS E TECNOLÓGICAS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL PROFMAT

APOSTILA DE PROPOSTAS DE ATIVIDADES PARA AULAS DE MATEMÁTICA NO ENSINO FUNDAMENTAL II E NO ENSINO MÉDIO BASEADAS EM TÉCNICAS DE CRIPTOGRAFIA

ISAC ROSA RODRIGUES

Produto final vinculado à dissertação de mestrado intitulada "**USO DE FERRAMENTAS DE CRIPTOGRAFIA NO ENSINO DE MATEMÁTICA NO ENSINO FUNDAMENTAL II E NO ENSINO MÉDIO: PROPOSTAS DE ATIVIDADES**" apresentada ao Programa de Mestrado profissional em Matemática em Rede Nacional – PROFMAT, da Universidade do Estado de Mato Grosso – UNEMAT, como requisito parcial para obtenção do grau de Mestre em Matemática, orientada pelo Prof. Dr. Raul Abreu de Assis e co-orientada pela profa. Dra. Luciana Mafalda Elias de Assis.

UNEMAT
Sinop-MT – 2024

Proposta de Atividades

Título	Apostila de Propostas de Atividades para Aulas de Matemática no Ensino Fundamental II e no Ensino Médio Baseadas em Técnicas de Criptografia
Nível de Ensino	Fundamental II e Médio.
Tipo de atividade	Expositiva e prática podendo ser em grupo ou individual dependendo dos materiais disponíveis e número de participantes.
Duração	5 aulas de 50 minutos para cada atividade proposta.
Objetivos	● Tornar a prática docente mais motivadora e rica de elementos desafiadores; ● Tornar a aula mais dinâmica e participativa, fazendo com que o aluno seja protagonista de seu aprendizado; ● Oportunizar ao estudante expor suas ideias e opiniões sobre a forma como o conteúdo de matrizes foi apresentado; ● Despertar o senso investigativo, bem como a curiosidade naquilo que se está aprendendo.
Conteúdos abordado	● Divisão euclidiana; aritmética modular; progressão aritmética. ● Matrizes e operações entre matrizes; ● Análise combinatória ● Estatística
Material utilizado	● Notebook para o professor; ● Chromebook para o aluno (verificar a disponibilidade na escola) e/ou outro computador que o aluno possa desenvolver as atividades ou celulares de uso pessoal dos alunos. ● Papel cartão para elaboração dos Citales.

SUMÁRIO

1 A cifragem por citale (ou cítala espartana) **04**
1.1 Atividades propostas 09
2 Cifragem por operações com matrizes **10**
2.1 Atividades propostas 14
3 Cifragem por transposição e cifragem por substituição **15**
3.1 Atividades propostas 23
4 Análise de frequência 24
4.1 Atividades propostas 35
5 Materiais de apoio. **37**

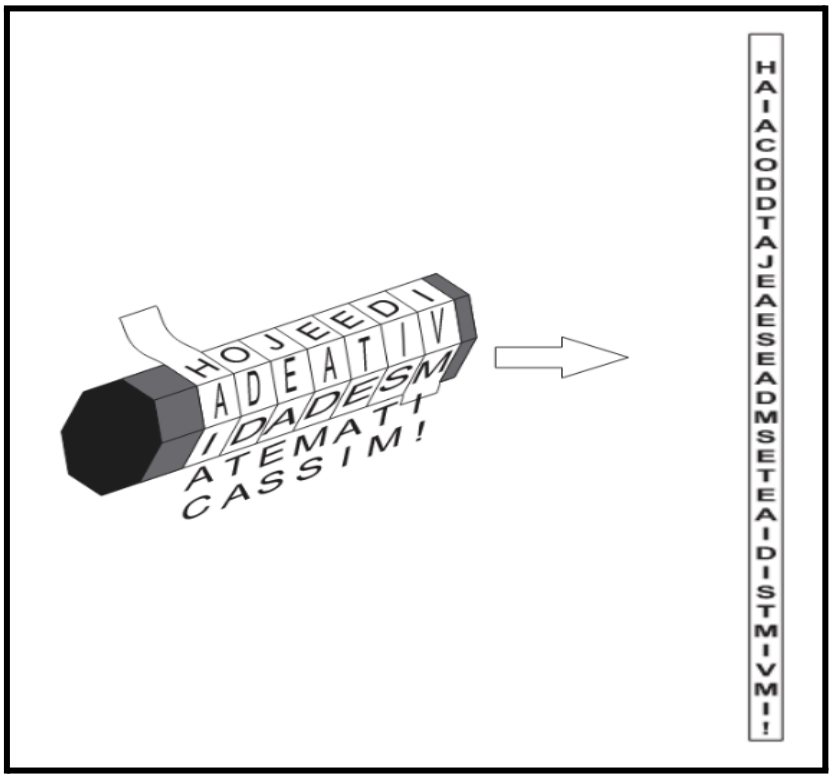
1. A CIFRAGEM POR CITALE (OU CÍTALA ESPARTANA)

Conteúdos relacionados: Divisão euclidiana; aritmética modular; progressão aritmética.

O citale é um aparelho simples para cifragem de mensagens que constitui em um prisma comprido ao redor do qual uma tira de couro, papel, pergaminho ou qualquer material base para escrita é enrolada e o texto a ser cifrado é escrito na tira no sentido longitudinal do citale, em seguida a tira é desenrolada e a sequência de caracteres obtidos ao longo da tira é o texto cifrado que pode ser enviado através do envio da própria tira ou ser transcrito em outro local. Normalmente, omitimos os espaços, acentuação e pontuação para que haja mais eficiência na cifragem. Observe o exemplo:

TEXTO ORIGINAL: Hoje é dia de atividades matemáticas? Sim!

Figura 1: Cifra do citale



Fonte: Elaborado pelo autor

RETIRANDO-SE ESPAÇOS, ACENTUAÇÃO E PONTUAÇÃO:
HOJEEDIADEATIVIDADESMATEMATICASSIM

Para simplificar o processo e a realização das atividades, os textos usados devem ser escritos de modo que ocupem por inteiro o último lado (chamaremos simplesmente de lado as faces retangulares do citale) utilizado do citale, ou seja, ou o número de caracteres do texto deve ser múltiplo do número de voltas dadas com a tira ao redor do citale, ou, ao final do texto, caso o último lado ocupado não tenha sido preenchido por completo, devemos inserir caracteres aleatórios até que todo espaço do último lado seja ocupado. As atividades propostas foram elaboradas considerando que este critério de simplificação tenha sido seguido.

TEXTO CIFRADO: HAIACODDTAJEAESEADMSETEAIDISTMIVMI

Outro detalhe é que não é obrigatório usar todos os lados do citale, no exemplo usamos um citale de 8 lados mas o texto só ocupou 5 desses lados, isso faz com que hajam espaços em branco na tira onde escrevemos o texto, o que dá indício do número de lados do citale utilizado, facilitando uma decifragem, para evitar tal fraqueza na cifragem é possível transcrever o texto cifrado para outro lugar eliminando-se os espaços em branco, uma outra abordagem nos permite manter o texto na tira, para isso basta preencher os lados não ocupados pelo texto com caracteres aleatórios que serão facilmente reconhecidas como um artifício de simples preenchimento de espaço por quem decifrar o texto.

O método básico de decifragem do citale é manter o texto na tira e enrolar esta em um citale idêntico ao que foi usado para cifrar o texto. Porém existem outros métodos, usados quando o texto é transcrito para outro lugar ou quando não se conhece as características do citale usado para cifrar o texto.

Se observarmos com atenção a estrutura do citale, podemos notar que as letras consecutivas no texto original estão sempre a uma mesma distância umas das outras no texto cifrado, dessa forma, se enumerarmos a posição de cada letra no texto cifrado, a divisão do número relativo a posição de letras consecutivas no texto original pelo número de lados do citale (seja tanto o número total de lados como o número de lados efetivamente utilizados), deixará um mesmo resto e assim, o texto poderá ser decifrado desde que identifiquemos o número de lados em questão.

Isso pode ser feito dividindo o número relativo à posição das letras no texto cifrado por algum número inteiro, agrupando aquelas cujos restos forem iguais e analisando se a sequência de letras obtidas faz algum sentido, caso não faça, repetimos o processo com outro número como divisor e vamos repetindo até encontrarmos o divisor adequado. Seguindo com nosso exemplo, enumeramos os caracteres do texto cifrado:

Tabela 1: Posição das letras no texto cifrado

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

H	A	I	A	C	O	D	D	T	A	J	E	A	E	S	E	A	D

19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	
M	S	E	T	E	A	I	D	I	S	T	M	I	V	M	I	

Fonte: Elaborado pelo autor

O menor número possível de lados para um prisma é 3, portanto esse será o primeiro número pelo qual dividiremos os números relativos às posições das letras no texto cifrado.

Nas tabelas a seguir escrevemos cada número relativo a posição de uma letra no texto cifrado na forma do teorema da divisão euclidiana, “r” indica o resto da divisão e “q” o quociente, iniciamos na tabela onde usamos o número 3 como divisor:

Tabela 2: Caracteres do texto e a divisão euclidiana da posição relativa pelo divisor 3

resto 1	resto 2	resto 0
H:1=0*3+1; r=1, q=0	A:1=0*3+2; r=2, q=0	I:1=1*3+0; r=0, q=1
A:4=1*3+1 r=1, q=1	C:5=1*3+2 r=2, q=1	O:6=2*3+0 r=0, q=2
D:7=2*3+1 r=1, q=2	D:8=2*3+2 r=2, q=2	T:9=3*3+0 r=0, q=3
A:10=3*3+1 r=1, q=3	J:11=3*3+2 r=2, q=3	E:12=4*3+0 r=0, q=4
A:13=4*3+1 r=1, q=4	E:14=4*3+2 r=2, q=4	S:15=5*3+0 r=0, q=5
E:16=5*3+1 r=1, q=5	A:17=5*3+2 r=2, q=5	D:18=6*3+0 r=0, q=6
M:19=6*3+1 r=1, q=6	S:20=6*3+2 r=2, q=6	E:21=7*3+0 r=0, q=7
T:22=7*3+1 r=1, q=7	E:23=7*3+2 r=2, q=7	A:24=8*3+0 r=0, q=8
I:25=8*3+1 r=1, q=8	D:26=8*3+2 r=2, q=8	I:27=9*3+0 r=0, q=9
S:28=9*3+1 r=1, q=9	T:29=9*3+2 r=2, q=9	M:30=10*3+0 r=0, q=10
I:31=10*3+1 r=1, q=10	V:32=10*3+2 r=2, q=10	M:33=11*3+0 r=0, q=11
I:34=11*3+1 r=1, q=11		

Fonte: elaborado pelo autor

Como teste, vamos agrupar algumas letras correspondentes ao resto 1:

1,4,7,10,13,16 => HADAAE

A sequência obtida não parece fazer muito sentido, portanto vamos testar usando o número 4 como divisor:

Tabela 3: Caracteres do texto e a divisão euclidiana da posição relativa pelo divisor 4

resto 1	resto 2	resto 3	resto 0
H:1=0*4+1 r=1, q=0	A:2=0*4+2 r=2, q=0	I:3=0*4+3 r=3, q=0	A:4=1*4+0 r=0, q=1
C:5=1*4+1 r=1, q=1	O:6=1*4+2 r=2, q=1	D:7=1*4+3 r=3, q=1	D:8=2*4+0 r=0, q=2
T:9=2*4+1 r=1, q=2	A:10=2*4+2 r=2, q=2	J:11=2*4+3 r=3, q=2	E:12=3*4+0 r=0, q=3
A:13=3*4+1 r=1, q=3	E:14=3*4+2 r=2, q=3	S:15=3*4+3 r=3, q=3	E:16=4*4+0 r=0, q=4
A:17=4*4+1 r=1, q=4	D:18=4*4+2 r=2, q=4	M:19=4*4+3 r=3, q=4	S:20=5*4+0 r=0, q=5
E:21=5*4+1 r=1, q=5	T:22=5*4+2 r=2, q=5	E:23=5*4+3 r=3, q=5	A:24=6*4+0 r=0, q=6
I:25=6*4+1 r=1, q=6	D:26=6*4+2 r=2, q=6	I:27=6*4+3 r=3, q=6	S:28=7*4+0 r=0, q=7
T:29=7*4+1 r=1, q=7	M:30=7*4+2 r=2, q=7	I:31=7*4+3 r=3, q=7	V:32=8*4+0 r=0, q=8
M:33=8*4+1 r=1, q=8	I:34=8*4+2 r=2, q=8		

Fonte: Elaborado pelo autor

Agrupando algumas letras correspondentes ao resto 1:

1,5,9,13,17,21 => HCTAAE

Novamente não há sentido aparente, vamos usar o 5 como divisor em um novo teste:

Tabela 4: Caracteres do texto e a divisão euclidiana da posição relativa pelo divisor 5

resto 1	resto 2	resto 3	resto 4	resto 0
H:1=0*5+1 r=1, q=0	A:2=0*5+2 r=2, q=0	I:3=0*5+3 r=3, q=0	A:4=0*5+4 r=4, q=0	C:5=1*5+0 r=0, q=1
O:6=1*5+1 r=1, q=1	D:7=1*5+2 r=2, q=1	D:8=1*5+3 r=3, q=1	T:9=1*5+4 r=4, q=1	A:10=2*5+0 r=0, q=2
J:11=2*5+1 r=1, q=2	E:12=2*5+2 r=2, q=2	A:13=2*5+3 r=3, q=2	E:14=2*5+4 r=4, q=2	S:15=3*5+0 r=0, q=3
E:16=3*5+1 r=1, q=3	A:17=3*5+2 r=2, q=3	D:18=3*5+3 r=3, q=3	M:19=3*5+4 r=4, q=3	S:20=4*5+0 r=0, q=4
E:21=4*5+1 r=1, q=4	T:22=4*5+2 r=2, q=4	E:23=4*5+3 r=3, q=4	A:24=4*5+4 r=4, q=4	I:25=5*5+0 r=0, q=5
D:26=5*5+1 r=1, q=5	I:27=5*5+2 r=2, q=5	S:28=5*5+3 r=3, q=5	T:29=5*5+4 r=4, q=5	M:30=6*5+0 r=0, q=6
I:31=6*5+1 r=1, q=6	V:32=6*5+2 r=2, q=6	M:33=6*5+3 r=3, q=6	I:34=6*5+4 r=4, q=6	

Fonte: Elaborado pelo autor

Agrupando algumas letras correspondentes ao resto 1:

1,6,11,16,21,26 => HOJEED

Agora, aparentemente temos uma palavra do texto original, para verificar se estamos no caminho correto ou se a palavra apareceu ao acaso, vamos agrupar em sequência as letras correspondentes aos restos 1,2,3,4 e 0:

Resto 1 => 1,6,11,16,21,26,31 => HOJEEDI
Resto 2 => 2,7,12,17,22,27,32 => ADEATIV
Resto 3 => 3,8,13,18,23,28,33 => IDADESM
Resto 4 => 4,9,14,19,24,29,34 => ATEMATI
Resto 0 => 5,10,15,20,25,30,35 => CASSIM

HOJEEDIADEATIVIDADESMATEMATICASSIM => Hoje é dia de atividades matemáticas? Sim!

É interessante notar que, se ao realizarmos as divisões, formos agrupando os resultados em células de tabelas cujo número de colunas for igual ao divisor usado,

quando usarmos o divisor correto o texto já estará decifrado se lermos as letras coluna por coluna como ocorreu na tabela 3, essa é uma característica que pode reduzir o trabalho da decifragem mas que pode não ser mencionada a fim de que os alunos tenham a oportunidade de notar tal detalhe. Seguindo essa abordagem, no momento em que os alunos realizarem as atividades propostas é aconselhável que os mesmos realizem cada divisão presente nas tabelas anteriores anotando os restos para que tenham a oportunidade de reconhecer os padrões que surgem. Após isso, é conveniente anotar em cada teste com determinado divisor apenas os números que já sabemos que deixarão o mesmo resto sem fazer as divisões uma a uma. Por exemplo: ao dividir os números naturais por 5 como foi feito na última tabela, já sabemos (e espera-se que os alunos percebam) que os números que deixarão resto 1 são os termos de uma *PA* de termo inicial 1 e razão 5: 1,6,11,16,21,26,31… os que deixarão resto 2 são os termos de uma PA de termo inicial 2 e razão 5: 2,7,12,17,22,27,32… e assim por diante. Isso se justifica justamente pelo caráter de repetição periódica da posição de letras consecutivas do texto original no texto cifrado. Se uma letra qualquer tem a posição x_1 no texto original e posição a_1 no texto cifrado e o citale utilizado para cifragem tem r lados, a próxima letra do texto original x_2 estará r posições à frente de x_1 no texto cifrado, enquanto x_3 estará r posições à frente de x_2, ou seja, se chamarmos de $P(x)$ a posição no texto cifrado de um caractere de posição genérica x no texto original, temos:

$$P(x_1) = a_1$$
$$P(x_2) = P(x_1) + r = a_1 + r$$
$$P(x_3) = P(x_2) + r = a_1 + 2r$$
$$\vdots$$
$$\vdots$$
$$P(x_n) = a_1 + (n-1)r$$

1. 1 ATIVIDADES PROPOSTAS:

01) A figura “citale de 7 lados” presente ao final desta apostila é a planificação de um citale de 7 lados, recorte-a nas linhas contínuas, faça as dobras nas linhas pontilhadas e cole as abas para montar um citale (aconselhamos colar a folha em uma cartolina ou similar antes de recortar para dar maior resistência). Use-o para decifrar o texto a seguir:

O N E P E S R S E E O U E A O T D D V M F L A E E A A A C S P A S I Z O G E M
C S E M I N A O N R T R D D M A - O A E U O D G D N N R S A A O D T E E N L S
O E C E O I A E S E L U L Q M D R E N E U T E U N I U E O L M A V G L R E C O
E A E N A A T R L S O I C I S I P D N H V O L L E D O E P E A L A D S A I

02) As sequências de letras a seguir são o resultado de uma cifragem por citale de uma frase. Em cada caso determine o número de lados do citale utilizado e a frase original:

a) B D A D V E O I T O O S M A O S C .

b) M A U L A T M G S O E U Q D C E U O O M E O N L M O V E M U E V E R
N A D O C S E Q E S R U R E A E Q E A E U M O N E B M T E O E R R R N
E A A O G P A S U R T U E O E M I V O A A A Q V Q D U E U E E Z E A E T
M M U E C I N R O Z A D N A O E S D T V E E I O G S N L U E H T I A A

03) Usando o citale construído na atividade (01) cifre algum texto não muito curto (em torno de 400 caracteres sem contar os espaços) e entregue a um colega enquanto ele lhe entrega um texto dele também cifrado. Determine um método de decifrar o texto rapidamente sem usar o citale e sem realizar todas as divisões realizadas no exemplo.

04) No texto foi recomendado que o último lado do citale ocupado pelo texto a ser cifrado fosse ocupado por completo, inclusive apesar da prática de se retirar a pontuação, um ponto de exclamação foi mantido no nosso exemplo devido a essa recomendação. Pense na estrutura do citale e do texto cifrado na tira que foi utilizada e indique um método de se contornar esse problema de modo que tal recomendação não precise ser seguida.

2. CIFRAGEM POR OPERAÇÕES COM MATRIZES

Conteúdos relacionados: Matrizes, operações com matrizes, conversão de dados alfabéticos para dados numéricos.

Nesta seção, apresentaremos como realizar uma cifragem utilizando operações entre matrizes. Iniciamos, verificando que uma mensagem qualquer pode ser organizada em tabelas. As letras e outros caracteres que formam um texto qualquer normalmente são dispostos em linhas, com o início do texto na esquerda da primeira linha superior e sua continuidade se dando para a direita e para as linhas que se seguem abaixo sendo este o sentido convencional de escrita e leitura (da esquerda para a direita e de cima para baixo) no Português e em diversos outros idiomas. Dessa forma é possível alinhar verticalmente os caracteres que compõem o texto em colunas de modo que cada linha tenha a mesma quantidade de caracteres (com a possível exceção da última). Observe um exemplo:

Frase na forma original:
O FUTURO NÃO É MAIS COMO ERA ANTIGAMENTE

Frase após o alinhamento (aqui consideramos o espaço entre palavras como um caractere representado por "_"):

Tabela 5: Caracteres da frase distribuídos em uma tabela 2x20

O	_	F	U	T	U	R	O	_	N	Ã	O	_	É	_	M	A	I	S	_
C	O	M	O	_	E	R	A	_	A	N	T	I	G	A	M	E	N	T	E

Fonte: Elaborado pelo autor

Podemos dizer que os elementos da frase formam uma tabela de 2 linhas e 20 colunas, se não nos importarmos em deixar partes de uma mesma palavra em linhas distintas podemos montar tabelas de diferentes números de linhas e colunas:

Tabela 6: Caracteres da frase distribuídos em uma tabela 4x10

O	_	F	U	T	U	R	O	_	N
Ã	O	_	É	_	M	A	I	S	_
C	O	M	O	_	E	R	A	_	A
N	T	I	G	A	M	E	N	T	E

Fonte: Elaborado pelo autor

Se associarmos um número distinto a cada caractere distinto usado na escrita, podemos converter um texto em uma sequência de números e, em seguida, a sequência de números em uma tabela, obtendo assim uma matriz de entradas numéricas. Se, por exemplo, definirmos as seguintes correspondências entre letras e números:

Tabela 7: Correspondência entre caracteres textuais e numéricos

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

21	22	23	24	25	26	27
U	V	W	X	Y	Z	_

Fonte: Elaborado pelo autor

A Tabela 6, pode ser convertida na seguinte matriz:

$$M = \begin{bmatrix} 15 & 27 & 6 & 21 & 20 & 21 & 18 & 15 & 27 & 14 \\ 1 & 15 & 27 & 5 & 27 & 13 & 1 & 9 & 19 & 27 \\ 3 & 15 & 13 & 15 & 27 & 5 & 18 & 1 & 27 & 1 \\ 14 & 20 & 9 & 7 & 1 & 13 & 5 & 14 & 20 & 5 \end{bmatrix}$$

Tendo convertido nosso texto em uma matriz, é possível cifrá-lo usando alguma operação que receba cada número da matriz e retorne um novo número. Evidentemente isso só fará sentido se usarmos alguma operação que possa ser "desfeita" para que o texto possa ser decifrado posteriormente. Multiplicar a matriz por algum escalar seria uma possibilidade, porém resultaria em uma cifragem fraca, assim, vamos optar pela multiplicação da nossa matriz por uma outra. A operação inversa (que desfaz) a multiplicação de uma matriz qualquer A por uma outra matriz B é a multiplicação da matriz resultante pela inversa de *B*, denotada como B^{-1} (BOLDRINI, 1986). Portanto, se encontrarmos uma matriz que possa ser multiplicada pela matriz do nosso exemplo (a multiplicação de matrizes somente está definida para casos específicos) e que seja invertível (nem toda matriz possui matriz inversa) podemos usar a multiplicação de matrizes para cifrar nosso texto.

Tendo definido nossa técnica de cifragem, as propriedades das matrizes nos impõe duas limitações: primeiramente, como a multiplicação de matrizes não é comutativa a ordem em que realizamos essa operação é fundamental para o sucesso da técnica, devemos portanto multiplicar nossa matriz por uma matriz inversível (que daqui em diante será chamada de chave) para cifrar o texto, e para decifrar devemos multiplicar a matriz obtida na cifragem pela inversa da chave exatamente nessa ordem para cifragem e decifragem. A segunda limitação resulta do fato de que só possível multiplicar matrizes quando uma delas (dita a primeira) tem o número de colunas igual ao número de linhas da outra (dita a segunda), portanto devido à ordem da multiplicação na cifragem nossa matriz deve ter o mesmo número de colunas que o número de linhas da chave e portanto a conversão do texto em matriz e a criação da chave devem resultar em matrizes que obedeçam esse quesito.

Ao exemplificar a conversão de texto em números e a criação de matrizes com esses dados obtivemos a seguinte matriz 4x10. Para cifrar o texto nesse caso, seria necessário uma chave com 10 linhas, como apenas matrizes quadradas possuem inversas (mas não necessariamente todas) teríamos portanto uma chave de ordem 10. Como o processo de multiplicação de matrizes aumenta consideravelmente o número de passos conforme o número de colunas da primeira matriz (e consequentemente o número de linhas da segunda) aumenta, é conveniente distribuir nossos dados em uma matriz com menor número de colunas, o que também nos facilitará a criação da chave. Para nosso exemplo vamos distribuir nossos dados em uma matriz 10x4 (para aplicar aos alunos é aconselhável usar uma matriz com um número ainda menor de colunas, para o caso do nosso texto poderia ser utilizada uma matriz 20x2 por exemplo):

$$\begin{bmatrix} 15 & 27 & 6 & 21 \\ 20 & 21 & 18 & 15 \\ 27 & 14 & 1 & 15 \\ 27 & 5 & 27 & 13 \\ 1 & 9 & 19 & 27 \\ 3 & 15 & 13 & 15 \\ 27 & 5 & 18 & 1 \\ 27 & 1 & 14 & 20 \\ 9 & 7 & 1 & 13 \\ 5 & 14 & 20 & 5 \end{bmatrix}$$

Agora precisamos obter como chave uma matriz de ordem 4 invertível, com algumas contas é possível verificar que a seguinte matriz atende à nossa necessidade:

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

A multiplicação de nossa matriz pela chave resulta:

$$\begin{bmatrix} 15 & 27 & 6 & 21 \\ 20 & 21 & 18 & 15 \\ 27 & 14 & 1 & 15 \\ 27 & 5 & 27 & 13 \\ 1 & 9 & 19 & 27 \\ 3 & 15 & 13 & 15 \\ 27 & 5 & 18 & 1 \\ 27 & 1 & 14 & 20 \\ 9 & 7 & 1 & 13 \\ 5 & 14 & 20 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 42 & 60 & 75 & 48 \\ 53 & 72 & 69 & 71 \\ 43 & 31 & 45 & 44 \\ 67 & 72 & 58 & 94 \\ 47 & 74 & 82 & 66 \\ 31 & 56 & 58 & 44 \\ 46 & 42 & 25 & 64 \\ 61 & 49 & 55 & 75 \\ 23 & 22 & 34 & 24 \\ 30 & 59 & 44 & 50 \end{bmatrix}$$

A sequência numérica obtida com a matriz resultante é a mensagem cifrada que pode ser enviada com relativa segurança a um determinado destinatário que conheça a matriz chave e portanto seja capaz de usar sua inversa para decifrar a mensagem através da obtenção da matriz original.

Um detalhe interessante é que muitos dos elementos da matriz obtida na cifragem são números que não aparecem na tabela de correspondência entre caracteres e números. Portanto, alguém que interceptasse a mensagem, mesmo conhecendo a correspondência entre letras e números sequer seria capaz de atribuir letras aos números que compõem a mensagem cifrada, impossibilitando o mesmo de aplicar alguma técnica de decifragem baseada na frequência dos caracteres.

Caso seja de interesse do professor, os cálculos das operações matriciais podem ser realizados pelos alunos com o auxílio de *softwares* específicos para tal. Uma opção indicada é a calculadora online e gratuita de matrizes disponível em: https://matrixcalc.org/, outra ferramenta que pode ser utilizada é o editor de planilhas Microsoft Excel.

2. 1 ATIVIDADES PROPOSTAS:

01) Durante a explicação do método foi afirmado, sem demonstração, que a chave proposta atenderia às nossas necessidades (ser invertível) e que era fácil verificar isso com algumas contas. Faça tal verificação.

02) Encontre a matriz inversa da matriz chave utilizada no exemplo do texto e multiplique a matriz resultante pela matriz que você encontrou. Confira se o resultado é a matriz original que havíamos multiplicado pela matriz chave.

03) Considerando que, após a definição de uma matriz chave, haja a intenção de utilizá-la para cifrar outros textos, a matriz formada pelos dados numéricos do novo texto a ser cifrado deve ter o número de colunas igual à ordem da matriz chave. Entretanto, é possível que o número de caracteres do novo texto não seja múltiplo da ordem da matriz chave. Como isso interfere no processo de cifragem?

04) Encontre métodos para contornar a situação descrita acima.

05) A sequência numérica a seguir resultou de um texto cifrado pelo método que vimos nos exemplos, utilizando a mesma tabela de associação entre caracteres e números e a mesma chave. Use a matriz inversa encontrada na atividade (02) e decifre o texto:

56	58	70	71	42	41	35	56	22	64	53	38	45
59	36	72	55	86	72	82	50	73	68	70	28	44
37	36	70	95	97	95	42	41	35	56	42	41	35
56	42	41	35	56	22	64	53	38	45	59	36	72
64	95	90	91	43	71	75	58	55	60	34	82	17
36	24	30	59	41	63	64	39	44	55	43	45	23
39	46	38	34	27	50	57	82	86	74	36	80	67
58	62	58	72	75	59	58	72	72	34	61	64	49

06) Encontre uma matriz de ordem 3 que atenda às propriedades necessárias para que possa ser usada como chave para cifragem. Forneça essa matriz a algum colega para que ele a utilize para cifrar um texto qualquer que você não conheça, receba a sequência numérica obtida pelo seu colega com o uso da sua chave e decifre o texto:

07) Analise com atenção todos os passos da cifragem por multiplicação de matrizes. Procure determinar ao menos um meio de tornar a cifragem mais forte (mais difícil de ser decifrada):

3. CIFRAGEM POR TRANSPOSIÇÃO E CIFRAGEM POR SUBSTITUIÇÃO

Conteúdos relacionados: Princípio fundamental da contagem; análise combinatória.

A cifragem por citale e alguns outros métodos específicos de cifragem pertencem a um grupo geral de cifras chamadas cifras de transposição. Esse tipo é caracterizado por uma troca da posição dos caracteres do texto original no texto cifrado, ou seja, cada letra de uma frase por exemplo, estará em uma posição diferente no texto cifrado daquela em que se encontrava no texto original porém nessa nova posição ela mantém sua identidade, ou seja é a mesma letra. Cifras desse grupo têm características de tratamento de caracteres opostas às do grupo chamado cifras de substituição, nas quais os caracteres mantém sua posição inalterada durante a cifragem, porém são trocados por outros caracteres de acordo com alguma pré-determinação. Um exemplo desse segundo grupo é cifragem por multiplicação de matrizes onde inicialmente cada letra do texto original é trocada por um número que mantém nesse estágio da cifragem a posição da letra à qual ele foi associado, depois cada número é trocado por outro obtido da multiplicação de matrizes porém a posição desse outro número no texto cifrado é a mesma do número anterior e consequentemente da letra do texto original.

❖ Cifragem por transposição:

Nas cifras de transposição temos efetivamente como resultado um anagrama do texto original, anagrama é um termo normalmente usado para se referir à palavras compostas exatamente pelas mesmas letras cada qual na mesma quantidade mas em ordem diferentes. Por exemplo, a palavra bola é um anagrama da palavra loba e a palavra socar é um anagrama da palavra rocas. Qualquer combinação nova das letras originais é um anagrama sem que seja necessário que a nova combinação tenha algum sentido textual, assim ablo e ocsar também são anagramas de loba e rocas respectivamente. É possível cifrar qualquer texto apenas gerando um anagrama qualquer do mesmo, e isso possibilita um número de diferentes cifragens que aumenta rapidamente conforme se aumenta o número de caracteres do texto.Observe:

- uma palavra de 2 letras só possui 2 anagramas:
  ai/ia;
  ou/uo

- uma palavra de 3 letras possui 6 anagramas:
  foi/fio/ofi/oif/ifo/iof
  olá/oal/loa/lao/alo/aol

- uma palavra de 4 letras possui 24 anagramas:
  beco/beoc/boce/boec/bcoe/bceo/ebco/eboc/ecbo/ecob/eocb/eobc/
  cebo/ceob/cbeo/cboe/cobe/coeb/oceb/ocbe/oecb/oebc/obce/obec

É notável que a cada letra que adicionamos à palavra, o número de anagramas possíveis é o número de anagramas para a quantidade anterior de letras vezes o número de letras atual. Isso se deve ao fato de que o números de anagramas é o número de permutações simples possíveis para dada quantidade de letras, logo para uma palavra de *n* letras temos *n!* anagramas possíveis. Observe, porém, que entre todos os anagramas possíveis podemos ter alguns repetidos caso hajam letras repetidas na palavra, o que certamente acontecerá caso queiramos formar anagramas de uma frase ou um texto, observe um exemplo com a palavra uau, onde enumeramos cada letra com um índice para facilitar a distinção entre o primeiro “u” e o segundo:

$u_1a_2u_3/u_1u_3a_2/a_2u_3u_1/a_2u_1u_3/u_3a_2u_1/u_3u_1a_2$

Temos, como era de se esperar, 6 anagramas para uma palavra de 3 letras porém apenas 3 anagramas distintos. Como, para uma palavra, frase ou texto qualquer, temos um número específico de possíveis anagramas que corresponde ao número de possíveis cifragens por transposição. Entretanto é evidente que a elaboração de dois textos cifrados que sejam iguais, a partir de um mesmo texto original não tem sentido lógico, devemos distinguir o número de cifras de transposição possíveis dos números de cifras de transposição que resultam em textos distintos.

É evidente que, apesar do número de cifragens por transposição ser altíssimo para textos que possuem um número alto de caracteres, na prática, a cifragem não pode ser feita de qualquer modo aleatório pois isso impossibilitaria a decifragem posterior. Assim, devemos cifrar um texto por transposição através de algum método bem definido de cifragem, como o citale. Nesses casos, a cifra definida para transpor os caracteres pode ser representada matematicamente por uma função bijetiva sobre o conjunto das posições do caractere no texto, enquanto que o processo de decifragem é a correspondente função inversa.

Algumas cifras simples de transposição:

- Cifra das colunas:

Nessa cifra os caracteres do texto a ser cifrado são escritos em colunas formando uma grade com um número de linhas pré definido, quando o número de linhas é atingido em uma coluna a escrita continua na coluna seguinte, ao final, caso a última coluna não seja inteiramente preenchida é possível inserir caracteres aleatórios para completar a grade. A mensagem cifrada é formada pelos caracteres na ordem em que ficam dispostos nas linhas da grade. Por exemplo, para uma grade com 4 linhas a frase “Não revele essa mensagem” é escrita assim na grade:

N	E	E	A	S	M
A	V	E	M	A	R
O	E	S	E	G	T
R	L	S	N	E	I

E portanto, cifrada assim:

N E E A S M A V E M A R O E S E G T R L S N E I

Para decifrar a mensagem basta que o destinatário conheça o número fixo de linhas utilizadas na grade e divida o número de caracteres da mensagem por esse número obtendo assim o número de colunas nas quais ele deve distribuir os caracteres da mensagem cifrada escrevendo-os linha por linha e finalmente lendo coluna por coluna. Essa cifra é muito semelhante a do citale, porém sem a necessidade de um objeto físico para realizar a cifragem. Especificamente, se fizermos um processo análogo à cifra das colunas, porém distribuindo os caracteres em linhas numa grade com o número de colunas fixo obteremos exatamente uma cifra por citale.

- Cifra por transposição de colunas

Nesta cifra, uma palavra chave é escrita na primeira linha de uma grade e, em seguida, a mensagem a ser cifrada é escrita abaixo, linha por linha com um total de colunas igual ao número de letras da palavra chave. A mensagem cifrada é obtida através da transcrição das colunas por ordem alfabética das letras da palavra chave. Por exemplo, para cifrar a mensagem “alguns infinitos são maiores que outros” usando a palavra chave “cifra”, a grade é escrita como:

C I F R A
A L G U N
S I N F I
N I T O S
S A O M A
I O R E S
Q U E O U
T R O S A

Como o anagrama da palavra chave em que as letras estão em ordem alfabética é ACFIR, escrevendo as letras da coluna de cada uma dessas letras temos:

Coluna do A: N I S A S U A
Coluna do C: A S N S I Q T
Coluna do F: G N T O R E O
Coluna do I: L I I A O U R
Coluna do R: U F O M E O S

E a mensagem cifrada será:

N I S A S U A A S N S I Q T G N T O
R E O L I I A O U R U F O M E O S

Para decifrar a mensagem, basta que o destinatário conheça a palavra chave utilizada na grade e divida o número de caracteres da mensagem pelo número de letras da palavra chave. Dessa forma, ele obtém o número de linhas nas quais ele deve distribuir os caracteres da mensagem cifrada, escrevendo-os então, coluna por coluna abaixo de cada letra da palavra chave na ordem alfabética das mesmas e, finalmente, lendo linha por linha.

- Cifras das espirais

Este é um conjunto de cifras que são na verdade variações de uma mesma ideia: escreve-se os caracteres da mensagem a ser cifrada em uma grade retangular como nas cifras anteriores. Em seguida, obtêm-se o texto cifrado transcrevendo os caracteres na ordem em que aparecem segundo uma “espiral

retangular” construída sobre a grade. Por exemplo, para cifrar a frase “cifras das espirais” podemos escrever os caracteres da mensagem linha por linha numa grade retangular e transcrevê-los para a mensagem cifrada segundo uma espiral retangular iniciada no canto superior direito e direcionada para o centro da grade no sentido anti-horário, assim:

As inúmeras variações dessa ideia podem ser obtidas pelas combinações das diferentes opções da distribuição dos caracteres na grade com as diferentes opções de construção da espiral:

1. a mensagem pode ser escrita na grade linha por linha ou coluna por coluna.
2. a espiral pode ser construída em sentido horário ou anti-horário.
3. a espiral pode ser construída das bordas para o centro ou do centro para as bordas.
4. a espiral pode iniciar (quando construída da borda para o centro) ou terminar (quando construída do centro para a borda) em qualquer um dos quatro vértices da grade.

❖ Cifragem por substituição:

Quando se trata da cifragem por substituição o número possível de cifras deixa de depender do número de caracteres do texto e passa a depender do número de caracteres existentes que podem ser usados para substituir os originais. Em teoria, o número de possíveis cifragens de qualquer texto por substituição é infinito visto que existem infinitos caracteres que podem ser usados como substitutos dos originais (uma prova disso é a troca de letras por números, como existem infinitos números, qualquer sequência textual pode ser convertida em infinitas sequências numéricas). Evidentemente, assim como na cifragem por transposição, na cifragem por substituição é necessário que o destinatário conheça de antemão o método de substituição específico usado em uma mensagem para que possa decifrá-la.

Algumas cifras simples de substituição:

- Cifra de César

Na chamada cifra de César cada letra do texto original é trocada por uma letra que se encontra à uma certa quantidade de posições à frente ou antes dessa letra no alfabeto. Por exemplo, podemos cifrar uma frase trocando cada letra da mesma pela letra que se encontra 3 posições à frente no alfabeto, a letra A por exemplo seria trocada pela letra D, a letra M pela letra P e a letra X pela letra pela

letra A, de um modo geral para essa configuração associamos as letras do alfabeto convencional por letras do alfabeto com deslocamento de 3 posições:

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
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

Seguindo esta mesma ideia, podemos definir outras cifras distintas, obtidas dos possíveis deslocamentos do alfabeto. Usando um deslocamento de 8 posições por exemplo, podemos cifrar a frase “existem várias possibilidades” através da seguinte relação:

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
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

Obtendo:

M F Q A B M U D I Z Q I A X W A A Q J Q T Q L I L M A

Além dos diferentes deslocamentos do alfabeto da cifra em relação ao original, é possível definir alfabetos “fora de ordem” por meio de permutações das letras do alfabeto original e usar esses “rearranjos” como base para a substituição, isso gera um número altíssimo de cifras distintas.

- Cifra de deslocamento por palavra chave

Uma cifra de substituição bastante interessante por, tal qual a cifra de César, ser de fácil implementação é a cifra de deslocamento por palavra chave. Nela, uma palavra chave (ou frase) é pré definida e o alfabeto cifrado será iniciado pelas letras da palavra chave, desconsiderando letras repetidas (e espaços caso se use uma frase), o restante do alfabeto cifrado é composto simplesmente pelas letras que não constam na palavra chave, as quais podem ser colocadas em ordem, ou assim como no caso da cifra de César, podemos ainda rearranjar as letras restantes. Por exemplo, se usarmos a palavra chave “criptografia”, retirando as letras repetidas obtemos a sequência C R I P T O G A F que iniciará nosso alfabeto para a cifragem, se mantermos as letras restantes em ordem obtemos:

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

Um exemplo usando a mesma palavra chave, porém rearranjando a letras restante:

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

A frase “os resultados podem variar” cifrada por (I), fica:

K Q N T Q U E S C P K Q L K P T H V C N F C N

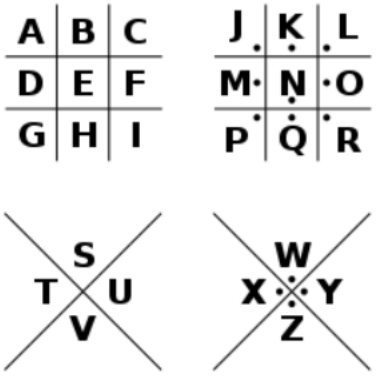
A mesma frase, cifrada por (II), fica:

Q W V T W Y L X C P Q W S Q P T M Z C V F C V

- Cifra do chiqueiro

A cifra do chiqueiro, também conhecida como cifra maçônica, por ter sido muito usada por maçons a partir do século XVII, substitui as letras do alfabeto por símbolos específicos através da associação em quatro grades geométricas como a seguinte:

Figura 02: Grades da cifra do chiqueiro



Fonte:https://pt.planetcalc.com/7842/ (acesso em 10/04/2024)

Assim como no caso da cifra de César, é possível obter um número elevado de distintas cifras do chiqueiro através da distribuição de um rearranjo do alfabeto

original nas grades. Usando a associação do exemplo anterior, a frase “use rearranjos” fica cifrada como:

Figura 03: Frase cifrada pela cifra do chiqueiro

Fonte: Elaborado pelo autor

- Código Morse

Apesar de não se tratar de uma cifra no sentido de um método criado para ocultar o significado de mensagens, o famoso código Morse se baseia na substituição de caracteres por símbolos específicos através de uma correspondência pré definida, o mesmo foi criado para o envio de mensagens por telégrafo e consiste em uma tabela de correspondência entre caracteres usuais e caracteres formados por específicas combinações de pontos e traços, como na figura abaixo:

Figura 04: Tabela de caracteres do código morse

A	•-	N	-•	0	-----
B	-•••	O	---	1	•----
C	-•-•	P	•--•	2	••---
D	-••	Q	--•-	3	•••--
E	•	R	•-•	4	••••-
F	••-•	S	•••	5	•••••
G	--•	T	-	6	-••••
H	••••	U	••-	7	--•••
I	••	V	•••-	8	---••
J	•---	W	•--	9	----•
K	-•-	X	-••-	.	•-•-•-
L	•-••	Y	-•--	,	--••--
M	--	Z	--••	?	••--••

Fonte: https://www.significados.com.br/codigo-morse/ (acesso em 10/04/2024)

Atualmente, com o advento da internet, a comunicação por código morse não apresenta segurança alguma, pois o mesmo é facilmente identificado devido à aparência dos símbolos e a partir da identificação é possível obter a tabela de associação rapidamente em uma pesquisa online. Porém, antes de tal possibilidade se difundir, o código Morse podia ser usado como meio de criptografia (fraca) caso fosse desejável esconder uma mensagem de alguém que sabia-se não ser conhecedor do código.

- Barreira do idioma

O caso do código Morse, em que um meio de comunicação escrito não foi desenvolvido para ocultar mensagens, mas em determinadas circunstâncias acaba por fazê-lo, pode ocorrer com as escritas de algumas civilizações antigas que utilizavam outros conjuntos de símbolos (alfabetos) para representar os fonemas de seus idiomas. É possível (e há casos) que no decorrer da história humana, alguns idiomas sejam extintos e a leitura de sua escrita deixe de ser possível de modo direto devido a inexistência de indivíduos “alfabetizados” em tal idioma e de textos claramente escritos no idioma em questão e em outro conhecido. Nessas situações os textos deixados por tais civilizações estão, de certa forma, criptografados para os leitores da atualidade e os métodos para decifrá-los são os mesmos geralmente usados para textos intencionalmente criptografados. Com isso é possível realizar atividades de treino de cifragem e decifragem, contextualizadas com um componente histórico e linguístico através da associação do nosso alfabeto com os diferentes alfabetos conhecidos atualmente.

3. 1 ATIVIDADES PROPOSTAS:

01) Já comentamos no texto que o número de possíveis cifras por transposição de um texto de n caracteres é n!, porém que o números de possíveis textos cifrados distintos será menor que n! para textos originais que apresentem caracteres repetidos (o que obrigatoriamente acontecerá quando *n* for maior que o número de caracteres existentes em determinado idioma), suponha que certa frase tenha 6 caracteres, porém 1 deles é repetido 3 vezes. Qual o número de possíveis cifragens por transposição para esta frase? Qual o número de cifragens distintas por transposição para esta frase?

02) Qual é o número de distintas cifragens por transposição para a frase: “HOJE VAMOS APRENDER”?

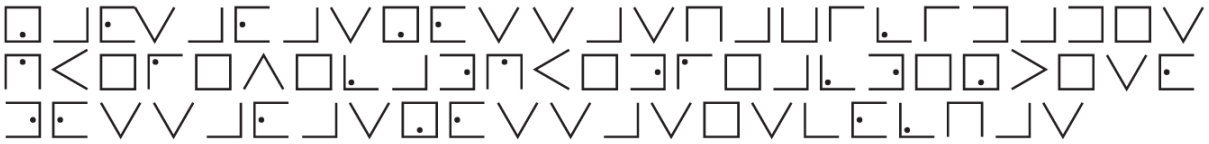
03) Considerando os quatro detalhes a respeito da distribuição de caracteres e construção da espiral na cifra das espirais, qual o total de cifras possíveis desse mesmo tipo para uma mesma frase?

04) Na cifra de César, na cifra de deslocamento por palavra chave e na cifra do chiqueiro (assim como em outras não abordadas aqui), é possível obter uma alto número de cifras utilizando diferentes rearranjos do alfabeto original. Na cifra de César, para o alfabeto latino (26 letras), quantas cifras distintas é possível obter por simples deslocamentos do alfabeto original? Quantas aproximadamente é possível obter através de rearranjos do alfabeto original?

05) Na cifra de deslocamento por palavra chave, se usarmos, como nos exemplos anteriores, a palavra chave CRIPTOGRAFIA, quantas cifras distintas podemos obter a partir de rearranjos do restante das letras do alfabeto?

06) Escolha uma palavra chave (ou frase) e calcule o número de cifras distintas disponíveis a partir de rearranjos do restante das letras do alfabeto:

07) Use as grades de associação da cifra do chiqueiro para decifrar a seguinte mensagem:



4. ANÁLISE DE FREQUÊNCIA

Conteúdos relacionados: Frequência; porcentagem; análise linguística, método hipotético-dedutivo.

A análise de frequência é uma técnica usada em criptoanálise para quebrar cifras de substituição. Em todas as cifras de substituição que vimos até o momento, cada caracter de um texto original é trocado por um único caractere específico no texto cifrado. O conjunto de caracteres usados na cifra constitui o que chamamos de alfabeto cifrado e como, nesses casos, temos um único alfabeto cifrado, tais cifras são chamadas de cifras de substituição monoalfabéticas.

As cifras monoalfabéticas sofrem de uma fraqueza muito grande devido à característica presente em qualquer linguagem escrita de que algumas letras são muito mais frequentes que outras ao longo de textos, isso é verdade em qualquer idioma e não apenas para letras como para determinadas combinações de letras em sequência e para palavras. Por exemplo, em português, a letra “A” é a mais comum, ou seja, a mais abundante em textos em comparação com as outras letras do alfabeto, sendo seguida pelas letras “E”, “O”, “S” e “R”, a abundância ou carência de determinadas letras é determinada por frequências relativamente constantes em textos de um mesmo idioma desde que tais textos sejam longos o suficiente. Dessa forma, como em uma cifra de substituição monoalfabética cada caracter é substituído sempre por um mesmo caracter no texto cifrado, as frequências relativas são preservadas. Assim, desde que se conheça o idioma no qual o texto original foi escrito e as frequências relativas das letras nesse idioma, é razoável supor que o caractere mais frequente do texto cifrado esteja substituindo a letra mais frequente do idioma, o segundo caracter mais frequente esteja substituindo a segunda letra mais frequente e assim por diante.

É evidente que, para letras de baixa frequência, ou letras de frequência parecida as hipóteses sobre quais caracteres as substituem não serão tão certeiras,

mas, desde que se use as informações mais distintas de frequências, e se decifre ao menos algumas partes do texto, o contexto extraído dessas partes já decifradas pode ser usado como auxílio no processo de decifrar as partes restantes. Por exemplo, se um determinado caractere em um longo texto cifrado que sabe-se que foi escrito originalmente em português aparece com maior frequência que todos os outros e supõe-se que o texto tenha sido cifrado por substituição monoalfabética, podemos supor com boa segurança que esse caractere está substituindo a letra “A”. Além disso, se, em algumas partes do texto esse caractere está seguido de um outro cuja frequência seja parecida com a das letras “H” e “Q” (que possuem frequências bem próximas no português) podemos determinar com relativa confiança que esse caracter é um substituto da letra “Q” ao nos atentarmos que em português a letra “A” é bem mais frequentemente seguida pelo “Q” do que pelo “H”. Percebemos que um conhecimento em linguística é um importante aliado na análise de frequência, muitos outros fatores característicos do idioma podem ser levados em consideração na análise, se em um texto cifrado os espaços entre as palavras foram mantidos. É possível, por exemplo, analisar as probabilidades das palavras desse idioma começar e terminar com determinadas letras e usar essas informações para auxiliar a análise de frequência. Abaixo segue uma tabela de frequência das letras do alfabeto em textos em português:

Figura 05: Frequência relativa das letras em textos em português

Letra	Freqüência		Letra	Freqüência
A	14.63%		N	5.05%
B	1.04%		O	10.73%
C	3.88%		P	2.52%
D	4.99%		Q	1.20%
E	12.57%		R	6.53%
F	1.02%		S	7.81%
G	1.30%		T	4.34%
H	1.28%		U	4.63%
I	6.18%		V	1.67%
J	0.40%		W	0.01%
K	0.02%		X	0.21%
L	2.78%		Y	0.01%
M	4.74%		Z	0.47%

Fonte: https://www.gta.ufrj.br/grad/06_2/alexandre/criptoanalise.html#:~:text=As%20vogais%20A%2C%20E%2C%20I,4%20dos%20textos%20em%20Portugu%C3%AAs. (acesso em 17/06/2024)

Vejamos um exemplo de decifragem por análise de frequência onde sabemos que o texto original está em português e foi cifrado por substituição monoalfabética:

Texto cifrado (para simplificação os espaços entre palavras foram mantidos):

xitidzia aiw vi uqvpi vili pcuqtlm wxqvqiw vwaai qvmaowbidmt nwvbm lm uioqi kixihma lm kicaiz ozivlma awnzqumvbwa m biujmu lm zmumlqi twa

Se contarmos os caracteres do texto obtemos os seguintes valores:

i: 20 vezes ≃ 17%
m: 14 vezes ≃ 12%
a: 11 vezes ≃ 9,5%
v: 9 vezes ≃ 7,8%
w: 9 vezes ≃ 7,8%
q: 8 vezes ≃ 6,9%
l: 7 vezes ≃ 6%
u: 7 vezes ≃ 6%
z: 5 vezes ≃ 4,3%
b: 4 vezes ≃ 3,4%
t: 4 vezes ≃ 3,4%
x: 3 vezes ≃ 2,6%
o: 3 vezes ≃ 2,6%
c: 2 vezes ≃ 1,7%
d: 2 vezes ≃ 1,7%
k: 2 vezes ≃ 1,7%
n: 2 vezes ≃ 1,7%
p: 2 vezes ≃ 1,7%
h: 1 vez ≃ 0,9%
j: 1 vez ≃ 0,9%
e: 0 vezes ≃ 0%
f: 0 vezes ≃ 0%
g: 0 vezes ≃ 0%
r: 0 vezes ≃ 0%
s: 0 vezes ≃ 0%
y: 0 vezes ≃ 0%

Comparando as frequências no texto cifrado com as fornecidas pela tabela anterior, podemos supor com relativa segurança que a letra “i” está substituindo a letra “a” e que a letra “m” está substituindo a letra “e”, vamos trocar essas letras no texto cifrado:

xAtAdzAa aAw vA uqvpA vAlA pcuqtlE wxqvqAw vwaaA qvEaowbAdEt nwvbE lE uAoqA kAxAhEa lE kAcaAz ozAvlEa awnzquEvbwa E bAujEu lE zEuElqA twa

A terceira letra mais comum no texto cifrado é o “a” e no português é o “o”, podemos portanto supor que um seja substituto do outro, isso faz todo sentido se considerarmos apenas a frequência das letras, porém teríamos no texto a sequência de letras “ooa” na palavra “vwaaA” o que é muito incomum pois na maioria das

palavras com duplicação da letra “o” a letra seguinte é uma consoante ou já se trata do final da palavra (cooptar; cooperação; voo; coordenador; álcool; zoológico; enjoo; etc), esse detalhe torna pouco provável a hipótese de que o “a” substitui o “o”. Vamos supor, então, que ele seja um substituto para a quarta letra mais comum do português, o “s” nesse caso para a palavra mencionada teremos a tríade “ssa” que é muito comum no português, especificamente no fim de uma palavra como é nesse caso (nossa; vossa; possa; pressa; submissa; remessa; massa; essa; fossa; etc), trocando o “a” pelo “s” temos:

xAtAdzAS SAw vA uqvpA vAlA pcuqtlE wxqvqAw vwSSA qvESowbAdEt nwvbE lE uAoqA kAxAhES lE kAcSAz ozAvlES SwnzquEvbwS E bAujEu lE zEuElqA twS

Essa segunda abordagem parece fazer muito sentido devido a quantidade de vezes em que o “s” apareceu no final de palavras o que é frequente no português devido aos plurais. Vamos procurar agora pela letra que substitui o “o”, as próximas letras mais frequentes do texto cifrado são o “v” e o “w” cujas frequências são idênticas. Se supormos que o “v” esteja substituindo o “o” teremos a palavra “oa” que não faz sentido algum como palavra individual (em português “oa” é um sufixo) e a palavra “OAlA” que também não parece fazer sentido qualquer que seja a letra que introduzirmos no lugar do “l”, vamos então supor que o substituto do “o” seja o “w” o que a princípio não parece gerar contradições ou raridades linguísticas, fazendo a substituição temos:

xAtAdzAS SAO vA uqvpA vAlA pcuqtlE OxqvqAO vOSSA qvESoObAdEt nOvbE lE uAoqA kAxAhES lE kAcSAz ozAvlES SOnzquEvbOS E bAujEu lE zEuElqA tOS

Como já usamos a hipótese de que o “w” substitui o “o” vamos tentar definir que letra está sendo substituída pelo “v” no texto cifrado, já temos hipóteses para as 4 letras mais comuns no português, a quinta letra mais comum é o “r”, se supormos que o “v” seja seu substituto, Neste caso, teremos as palavras “ra” e “RAlA” que faz sentido supondo que o texto fale sobre rãs (ra seria rã sem a acentuação e rala pode ser raça caso o “l” esteja substituindo o “c”) porém teremos também a palavra ROSSA inexistente no português. Apesar da possibilidade de se tratar de um erro de ortografia para a palavra roça, vamos supor que não seja esse o caso. Analisaremos agora a hipótese de que o “v” seja um substituto para a sexta letra mais comum no português o “i”, nesse caso surge a palavra IOSSA, inexistente no português e a palavra IAlA, com o “l” ainda a ser trocado, as palavras obtidas pela substituição do “l” nessa última são consideravelmente raras, considerando essas duas observações vamos descartar essa hipótese. Finalmente podemos supor que o “v” seja um substituto para a sétima letra mais comum no português o “n”, nesse caso teremos algumas palavras bastante comuns como NOSSA, NA e as palavras possíveis de se obter substituindo o “l” em NAlA (nada, nata, naja), vamos seguir por este caminho e realizar a substituição:

xAtAdzAS SAO NA uqNpA NAlA pcuqtlE OxqNqAO NOSSA qNESoObAdEt nONbE lE uAoqA kAxAhES lE kAcSAz ozANlES SOnzquENbOS E bAujEu lE zEuElqA tOS

Agora vamos tentar identificar no texto as letras que substituem o “r” e o “i”. Supondo, inicialmente, que o “q” substitui o “r” teremos a palavra (parcialmente decifrada) RNESoObAdEt, e a dupla “RN” apesar de aparecer em várias palavras (discernimento, cerne, escárnio, adorno, etc) não aparece no início de palavras em português e portanto essa hipótese é bem improvável. Por outro lado partirmos da hipótese de que o “q” substitui o “i” não obtemos situações incomuns ou impossíveis para as sequências de letras que surgem, vamos então realizar tal substituição:

xAtAdzAS SAO NA uINpA NAlA pcuItlE OxINIAO NOSSA INESoObAdEt nONbE lE uAoIA kAxAhES lE kAcSAz ozANlES SOnzIuENbOS E bAujEu lE zEuEllA tOS

A próxima letra mais comum do texto cifrado é o “l” e a próxima hipótese razoável com base nas frequências é que ele seja um substituto para o “r”, porém isso nos dá a palavra “RE” (que pode ser a palavra ré sem a acentuação), aparecendo três vezes no texto, sendo essa uma palavra que normalmente é comum apenas em contextos musicais (nota ré) ou sobre manobras e movimentos orientados (marcha ré) é mais provável que o “l” substitua a próxima letra mais comum do português, a letra “d”, pois nesse caso a palavra que aparece três vezes será DE, uma preposição extremamente comum mesmo em textos curtos, a partir de tal hipótese temos:

xAtAdzAS SAO NA uINpA NADA pcuItDE OxINIAO NOSSA INESoObAdEt nONbE DE uAoIA kAxAhES DE kAcSAz ozANDES SOnzIuENbOS E bAujEu DE zEuEDIA tOS

Diferindo um pouco da distribuição de frequências de letras no português, em nosso texto o “r” evidentemente tem uma frequência mais baixa que o esperado. Vamos prosseguir procurando determinar qual letra o substitui nessa cifra, vamos supor que seja a próxima letra mais frequente em nosso texto o “u”, seguindo essa hipótese, temos:

xAtAdzAS SAO NA RINpA NADA pcRItDE OxINIAO NOSSA INESoObAdEt nONbE DE RAoIA kAxAhES DE kAcSAz ozANDES SOnzIRENbOS E bARjER DE zEREDIA tOS

Nesse caso o único indício forte de que podemos estar corretos é a palavra RINpA que pode ser RINHA, porém como isso é pouco para tomarmos uma decisão vamos supor que o substituto do “r” seja o “z” (próxima letra mais comum após o “u” em nosso texto cifrado) para essa hipótese temos:

xAtAdRAS SAO NA uINpA NADA pcuItDE OxINIAO NOSSA INESoObAdEt nONbE DE uAoIA kAxAhES DE kAcSAR oRANDES SOnRIuENbOS E bAujEu DE REuEDIA tOS

Nesse caso também temos um único indício forte de estarmos corretos, a palavra oRANDES que pode ser GRANDES, nesse ponto poderíamos escolher uma das hipóteses e continuar nossos testes porém se escolhermos o substituto errado para o “r”. Podemos gastar muito tempo e energia na decifragem antes de ficar evidente nosso erro, portanto vamos tentar melhorar nossas duas hipóteses supondo que entre as duas letras que analisamos “u” e “z” aquela que não for substituta do “r” será substituta do “m” a próxima letra mais frequente do português que ainda não analisamos, para essa abordagem nossas hipóteses nos dão:

HIPÓTESE I (r foi substituído por u e m foi substituído por z):

xAtAdMAS SAO NA RINpA NADA pcRItDE OxINIAO NOSSA INESoObAdEt nONbE DE RAoIA kAxAhES DE kAcSAM oMANDES SOnMIRENbOS E bARjER DE MEREDIA tOS

HIPÓTESE II (r foi substituído por z e m foi substituído por u):

xAtAdRAS SAO NA MINpA NADA pcMItDE OxINIAO NOSSA INESoObAdEt nONbE DE MAoIA kAxAhES DE kAcSAR oRANDES SOnRIMENbOS E bAMjEM DE REMEDIA tOS

Agora fica evidente que, ao menos entre essas duas hipóteses, a segunda é bem mais razoável, pois temos pela segunda hipótese a palavra REMEDIA, muito mais provável de ser parte do texto original que MEREDIA. Além disso, oRANDES obtido pela segunda hipótese pode ser, como já comentamos, a palavra GRANDES. Porém, para a primeira hipótese não temos letras que possam substituir a primeira letra de oMANDES de modo a fazer algum sentido. Pela análise dessa palavra em particular, também vemos que, na segunda hipótese, o “o” deve ser substituto do “g” o que condiz com a palavra MAoIA, que no caso será MAGIA. Portanto, vamos adotar a segunda hipótese e já adicionar a nova hipótese de que “o” substitui “g”:

xAtAdRAS SAO NA MINpA NADA pcMItDE OxINIAO NOSSA INESGObAdEt nONbE DE MAGIA kAxAhES DE kAcSAR GRANDES SOnRIMENbOS E bAMjEM DE REMEDIA tOS

Poderíamos continuar fazendo hipóteses baseadas em comparações das frequências de cada letra no texto cifrado e no português, porém a essa altura, já temos alguns indícios de quais são determinadas palavras (na verdade já tínhamos tais indícios alguns passos atrás, mas dei continuidade a análise de frequência para ilustrar melhor o método). Assim pode ser bem mais vantajoso elaborar as próximas

hipóteses a partir disso, principalmente porque as letras que faltam são aquelas pouco frequentes e algumas delas têm frequências muito parecidas. Por exemplo, a palavra parcialmente decifrada INESGObAdEt, muito provavelmente é INESGOTÁVEL, confiantes de que isso está correto, elaboramos a hipótese de que “b” substitui “t”, “d” substitui “v” e “t” substitui “l”, aplicando essa hipótese temos:

xALAVRAS SAO NA MINpA NADA pcMILDE OxINIAO NOSSA INESGOTAVEL nONTE DE MAGIA kAxAhES DE kAcSAR GRANDES SOnRIMENTOS E TAMjEM DE REMEDIA LOS

Agora, devido a primeira e sétima palavras do texto parece muito evidente que “x” substitui “p”, aplicando essa hipótese obtemos:

PALAVRAS SAO NA MINpA NADA pcMILDE OPINIAO NOSSA INESGOTAVEL nONTE DE MAGIA kAPAhES DE kAcSAR GRANDES SOnRIMENTOS E TAMjEM DE REMEDIA LOS

Pelas palavras nONTE e SOnRIMENTOS, temos que o “n” substitui o “f”, e encontramos:

PALAVRAS SAO NA MINpA NADA pcMILDE OPINIAO NOSSA INESGOTAVEL FONTE DE MAGIA kAPAhES DE kAcSAR GRANDES SOFRIMENTOS E TAMjEM DE REMEDIA LOS

Nesse momento já é bem notável pela palavra MINpA e o contexto em que está inserida que “p” substitui “h” o que nos leva a concluir por HcMILDE que “c” substitui “u” e consequentemente por kAUSAR que “k” substitui “c”:

PALAVRAS SAO NA MINHA NADA HUMILDE OPINIAO NOSSA INESGOTAVEL FONTE DE MAGIA CAPAhES DE CAUSAR GRANDES SOFRIMENTOS E TAMjEM DE REMEDIA LOS

Finalmente, decifrando o “h” como “z”, o “j” como ”b” e inserindo a pontuação e acentuação necessárias, temos o texto decifrado:

PALAVRAS SÃO NA MINHA NADA HUMILDE OPINIÃO, NOSSA INESGOTÁVEL FONTE DE MAGIA, CAPAZES DE CAUSAR GRANDES SOFRIMENTOS E TAMBÉM DE REMEDIÁ-LOS.

Aqui, cabem alguns comentários adicionais sobre o uso da análise de frequência: evidentemente apesar da ideia principal ser bastante simples, a aplicação eficiente envolve muito mais que uma simples comparação de frequências relativas, sendo importante um bom domínio e conhecimento de linguagem, a

habilidade de elaborar boas hipóteses com base em certa quantidade de dados além de testá-las e também, em diversos momentos um pouco de intuição.

Como vimos no exemplo anterior, as frequências de caracteres em um texto curto podem apresentar consideráveis divergências com as frequências do idioma, no nosso exemplo, o “r” era a nona letra mais frequente, enquanto de um modo geral no português ele é quinta. Essas divergências tendem a diminuir em textos mais longos, porém outro detalhe importante é que elas podem se manter ou até serem mais presentes quando analisamos textos relacionados a contextos muito específicos, um documento militar ou um artigo sobre biologia por exemplo, as frequências das letras podem diferir bastante do padrão observado em textos gerais, desse modo, alguém que procura decifrar um texto por análise de frequência, e que sabe que o conteúdo do texto cifrado pertence à um contexto específico, deve preferencialmente usar como base uma tabela de frequências de letras obtidas da análise de textos que também pertençam a esse mesmo contexto.

Outro detalhe é que, conforme avançamos na decifragem de um texto, podemos realizar testes de hipóteses mais gerais sobre o alfabeto cifrado utilizado. No nosso exemplo, depois de decifrar umas quatro ou cinco letras, poderíamos ter comparado a posição de cada letra do texto original no alfabeto com a posição da letra que o substituiu a fim de verificar se a cifra utilizada foi a cifra de César, se o fizéssemos, perceberíamos que, de fato, para cifrar este texto foi usada uma cifra de César com deslocamento de oito posições. Ao contrário de outros métodos de decifragem, percebemos que a análise de frequência pode ser bem flexível, combinando racionalidade e criatividade na hora de elaborar hipóteses. Portanto, ao aplicarmos esse método, caso um palpite lhe pareça uma boa opção de caminho, é interessante analisá-lo, pois, isso não lhe tomará muito tempo e se o palpite se mostrar correto, pode reduzir muito os esforços restantes na tarefa de decifrar o texto.

Para auxiliar nas atividades relacionadas a esse tópico é possível usar algoritmos em alguma linguagem de programação para realizar as tarefas de contagem de caracteres, substituição de um caractere por outro para testar as hipóteses e até mesmo para realizar uma cifragem após um alfabeto cifrado ser definido. No final desse material constam alguns algoritmos em linguagem python que podem ser copiados e colados em um ambiente de programação para a execução. Para a linguagem python existem editores onlines dispensando o download de softwares um exemplo é o encontrado no endereço https://programiz.pro/ide/python. Consta também um algoritmo para implementar a cifra descrita a seguir.

Devido à análise de frequência, qualquer cifra de substituição monoalfabética se torna bastante insegura. Uma das ideias desenvolvidas por criptógrafos para garantir a segurança no envio de mensagens foram as chamadas cifras de substituição polialfabéticas, nas quais, como o nome já indica, mais de um alfabeto cifrado é usado. É evidente que ao utilizar uma cifra de substituição polialfabética deve-se ter bem definido qual dos alfabetos será usado em cada parte do texto, a

fim de que a mensagem possa ser decifrada através de passos bem definidos. Para exemplificar, imagine que dois alfabetos cifrados sejam definidos como segue na tabela abaixo, onde na primeira linha temos o alfabeto padrão e nas seguintes os dois cifrados:

Tabela 08: Dois alfabetos cifrados

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

Fonte: Elaborado pelo autor

De posse de tais ferramentas podemos determinar uma cifra onde a primeira letra de um texto original é cifrada de acordo com o primeiro alfabeto, a segunda de acordo com o segundo, e de um modo geral letras de posição ímpar são cifradas pelo primeiro e as de posição par pelo segundo. O termo “cifra polialfabética” por exemplo, seria cifrado como “ebyxq tgvopsnqltdomq”. Algumas vantagens desse tipo de cifra ficam evidentes já com esse exemplo: a letra “a”, de maior ocorrência na palavra original foi cifrada por duas letras distintas reduzindo sua frequência na palavra cifrada, além de uma mesma letra na palavra original poder ser cifrada por duas letras distintas, uma mesma letra repetida na palavra cifrada pode estar cifrando duas letras distintas, como ocorre por exemplo com a letra “t” que em sua primeira aparição está cifrando a letra “p” e na segunda a letra “e”.

Um exemplo relativamente famoso de cifra polialfabética é a chamada cifra de Vigenère, que usa 26 alfabetos cifrados distintos, cada qual sendo obtido por um deslocamento distinto do alfabeto padrão (ou seja, cada um representa uma cifra de César), incluindo um que curiosamente é o próprio alfabeto padrão (deslocamento de zero posições). A partir de uma palavra, frase, ou sequência qualquer de letras (de preferência fácil de se memorizar) chamada chave, um alfabeto específico dentre os 26 é selecionado para cifrar cada letra do texto original. Vamos observar um exemplo para entender como especificamente a chave atua na escolha dos alfabetos cifrados. Para facilitar o uso de cada alfabeto no momento correto, é construída uma tabela contendo o alfabeto padrão na primeira linha e os alfabetos cifrados nas linhas seguintes, cada qual resultando do deslocamento por uma posição do alfabeto acima, essa tabela é chamada de tábua reta (ou tábula recta, como é mais encontrada na literatura relacionada), ou quadrado de Vigenère:

Figura 05: Quadrado de Vigenère

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

FONTE: https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=1831&id2=286 (acesso em 20/06/2024)

De posse do quadrado de Vigenère, escolhemos uma chave. Vamos usar a palavra “SOMA”, então associamos a primeira letra da chave com a primeira da mensagem, a segunda letra da chave com a segunda da mensagem e assim sucessivamente, quando as letras da chave acabarem (nesse caso na quarta letra) associamos a próxima letra da mensagem com a primeira da chave novamente e continuamos até que todas as letras da mensagem estejam associadas à uma letra da chave, um jeito prático de fazer isso é escrever a chave repetidas vezes acima da mensagem combinando as duas letra por letra, se quisermos cifrar a frase “não temo o que vem depois”, por exemplo, escrevemos:

PALAVRA - CHAVE: S O M A S O M A S O M A S O M A S O M A
MENSAGEM ORIGINAL: n ã o t e m o o q u e v e m d e p o i s

Agora, de acordo com a letra da chave escolhemos uma linha do quadrado, a linha que se inicia por essa letra e que define um dos 26 alfabetos, em seguida procuramos a intersecção dessa linha com a coluna iniciada pela letra correspondente na mensagem e usamos a letra dessa intersecção para cifrá-la, por exemplo, para o nosso caso, a primeira letras da chave é o “S” e a primeira letra da mensagem é o “n”, portanto, esse “n” será cifrado pela intersecção da linha iniciada pelo “S” (linha 18) com a coluna iniciada pelo “n”, nessa intersecção se encontra a letra “f” que portanto será a substituta do “n”, no próximo passo a letra da chave é o “O” que define a linha 14 e está relacionado com o “a” da mensagem na intersecção da linha 14 com a coluna do “a” encontramos a letra “o” que será a substituta do “a”, prosseguindo com o processo obtemos:

PALAVRA - CHAVE: S O M A S O M A S O M A S O M A S O M A
MENSAGEM ORIGINAL: n ã o t e m o o q u e v e m d e p o i s
MENSAGEM CIFRADA: f o a t w a a o i i q v w a p e h c u s

Como era de se esperar em um cifra polialfabética, uma mesma letra original foi cifrada por mais de uma letra e uma mesma letra cifrada representa mais de uma letra original. Como nossa chave tem 4 letras, alternamos no uso de 4 alfabetos cifrados, uma chave maior resultaria no uso de mais alfabetos tornando a cifra ainda mais segura.

Para decifrar, realizamos o processo inverso: associamos as letras da chave com as letras da mensagem cifrada, podemos escrever a chave acima da mensagem cifrada como fizemos para cifrar. A partir de cada letra da chave definimos uma linha do quadro e procuramos nessa linha a letra cifrada relacionada a letra da chave em questão, a letra que inicia a coluna onde a letra cifrada foi encontrada é a letra original. No nosso exemplo, iniciamos com a letra “S” que define a linha 18, nela procuramos a letra “f” e como a mesma se encontra na intersecção da linha 18 com a coluna do “n” então a letra original que foi cifrada como “f” é o “n”.

A abordagem padrão da técnica de análise de frequência não funciona contra a cifra de Vigenère, pois o uso de vários alfabetos disfarça a frequência das letras na mensagem, no nosso exemplo temos as seguintes frequências para as letras na mensagem original e na mensagem cifrada:

MENSAGEM ORIGINAL:

LETRA	o	e	m	n	a	t	q	u	v	d	p	i	s
OCORRÊNCIA	4	4	2	1	1	1	1	1	1	1	1	1	1

MENSAGEM CIFRADA:

LETRA	a	o	w	i	f	t	q	u	v	e	p	h	c	s
OCORRÊNCIA	4	2	2	2	1	1	1	1	1	1	1	1	1	1

Enquanto existem duas letras mais frequentes na mensagem original, na cifrada só há uma, o “a”, que, nesse caso, cifra duas letras distintas da mensagem original.

Apesar da segurança relativa da cifra de Vigenère (que inclusive foi conhecida por muitos anos como a cifra indecifrável), ainda é possível decifrá-la. Em um texto relativamente longo (quanto mais longo maior a chance do padrão mencionado a seguir ocorrer) é bem provável que determinadas palavras de alta ocorrência sejam cifradas em mais de um momento no texto pela mesma parte da chave e portanto resultem em sequências iguais de letras no texto cifrado, o espaço entre essas repetições dá ao criptoanalista uma noção do tamanho (número de letras) da chave utilizada, analisando diferentes repetições que surgem em textos longos é possível elaborar uma boa hipótese sobre esse tamanho da chave quando o espaçamento entre repetições distintas indicam um mesmo tamanho.

A partir dessa hipótese, é possível separar o texto em “blocos” das letras que se supõe terem sido cifradas a partir de uma mesma letra da chave, por exemplo: se as repetições indicam que a chave contém 7 letras, então a primeira, a oitava, a décima quinta letras do texto cifrado e todas as outras que estão deslocadas de um múltiplo de 7 a partir da primeira terão sido cifradas pela primeira letra da chave e portanto formam um bloco, da mesma forma a segunda letra do texto cifrado e todas as outras que estão deslocadas de um múltiplo de 7 a partir dela terão sido cifradas pela segunda letra da chave e formarão outro bloco, em cada bloco a frequência de letras segue o padrão normal e portanto nos blocos é possível aplicar a análise de frequência, como em cada bloco temos efetivamente as letras obtidas por uma cifra de César, a análise de frequência nos permite determinar o deslocamento do alfabeto cifrado usado em cada bloco e consequentemente a letra da palavra chave que determinou esse alfabeto, determinando a palavra chave podemos decifrar o texto facilmente como descrito anteriormente.

4. 1 ATIVIDADES PROPOSTAS:

01) Usando análise de frequência, decifre o texto a seguir, originalmente em português e cifrado por substituição monoalfabética:

QSOQL G GXZKG LQWT Q CTKRQRT RTKKQRTOKQ G GFZTD T IOLZGKOQ G QDQFIQ T XD DOLZTKOG DQL IGPT T XDQ RQROCQ HGK OLLG EIQDQ-LT HKTLTFZT.

02) Usando análise de frequência, decifre o texto a seguir, originalmente em português e cifrado por substituição monoalfabética:

T OVPOCT VLHTC TVUOKIO KL SLCDRLKBO, COMOHTKIL T MTVBT OWBOKVTL IO LUOTKLV TRNDV O VOCOKTV PHLCOVBTV. TV TMOV VLYCOMLTJ TV TCMLCOV, OKXNTKBL LV VLKV IT KTBNCORT COVVLTJ. T UTIT ZTVVL, LV OWZHLCTILCOV OKULKBCTJ T CDXNORT OVULKIDIT KTV TCOTV TDKIT KTL IOVYCTMTITV. L VLH, ULJ VON YCDHSL DKBOKVL, TXNOUO L VLHL TCDIL, ZCOZTCTKIL-L ZTCT TV VOJOKBOV XNO, OJ YCOMO, VOCTL ZHTKBTITV.

03) Usando análise de frequência, decifre o texto a seguir, originalmente em português e cifrado por substituição monoalfabética:

RI UBRI 7RUUZW TRU ZEOUZ HI TZLUHI, RXZUZ7ZELR UZ7PUIRI ZIIZE7BHBI THUH HI 7UBHOPUHI YPZ VHJBOHW ZIOZ WPELR. H IZUZEBLHLZ LR 7ZEHUBR Z YPZJUHLH HTZEHI TZQR 7HEOR LRI THIIHURI Z R WPUWPUBR LHI XRQVHI HR AZEOR. H VHUWREBH ZEOUZ H OZUUH Z RI IZUZI YPZ EZQH ABAZW Z ZABLZEOZ ZW 7HLH LZOHQVZ. ER 7RUHÇHR LHI IZQAHI, UZTQZOHI LZ ABLH Z WBIOZUBRI, RI ABH4HEOZI LZI7RJUZW VBIORUBHI HEOB3HI 3UHAHLHI EHI UR7VHI.

04) Realize uma análise de frequência no texto cifrado pela cifra do chiqueiro na atividade de número 07 do tópico anterior (III - CIFRAGEM POR TRANSPOSIÇÃO E CIFRAGEM POR SUBSTITUIÇÃO).

05) Em grupos, cifrem textos em português com pelo menos 80 palavras, usando substituição monoalfabética, troquem os textos entre os grupos e tentem decifrar o texto recebido através da análise de frequência.

06) Cifre um texto com a cifra de Vigenère, realize uma análise de frequência do texto cifrado e compare o resultado com a frequência das letras no texto original. Argumente sobre a eficiência da análise de frequência contra a cifra de Vigenère:

07) Em grupos, cifrem textos em português com pelo menos 80 palavras, usando a cifra de Vigenère, troquem os textos entre os grupos informando também a quantidade de letras da chave utilizada e tentem decifrar o texto recebido identificando qual é a chave através da análise de frequência nos blocos de letras obtidos do texto cifrado.

5. MATERIAIS DE APOIO:

- CÓDIGO EM PYTHON PARA CONTAR AS LETRAS E ALGARISMOS DE UM TEXTO:

```python
from collections import Counter
import re

def contar_letras(texto):
    # Normaliza o texto removendo acentos e convertendo para minúsculas
    texto_normalizado = re.sub(r'[áàâã]', 'a', texto.lower())
    texto_normalizado = re.sub(r'[éê]', 'e', texto_normalizado)
    texto_normalizado = re.sub(r'[í]', 'i', texto_normalizado)
    texto_normalizado = re.sub(r'[óôõ]', 'o', texto_normalizado)
    texto_normalizado = re.sub(r'[ú]', 'u', texto_normalizado)

    # Remove caracteres que não são letras ou números
    texto_normalizado = re.sub(r'[^a-z0-9]', '', texto_normalizado)

    # Conta a ocorrência de cada letra e número
    contagem_letras = Counter(texto_normalizado)

    return contagem_letras

# Exemplo de uso
texto = "INSIRA SEU TEXTO AQUI"
contagem = contar_letras(texto)

print(contagem)
```

Fonte: Elaborado pelo autor através do chatbot ChatGPT; versão: GPT 4o. Disponível em: https://chatgpt.com/ (acesso em 20/05/2024)

- CÓDIGO EM PYTHON PARA SUBSTITUIR UMA LETRA OU ALGARISMO AO LONGO DE UM TEXTO POR UMA LETRA ESPECIFICADA:

```python
def substituir_letra(texto, letra_antiga, letra_nova):
    # Substitui todas as ocorrências da letra antiga pela letra nova no texto
    texto_substituido = texto.replace(letra_antiga, letra_nova)
    return texto_substituido

# Exemplo de uso
```

```
texto = "INSIRA SEU TEXTO AQUI"
letra_antiga = 'INSIRA AQUI A LETRA OU ALGARISMO A SER SUBSTITUÍDO'
letra_nova = 'INSIRA AQUI A LETRA SUBSTITUTA'

# Normalizar o texto (removendo acentos, mas mantendo a capitalização)
import re

def normalizar(texto):
    texto_normalizado = re.sub(r'[ÁÀÂÃáàâã]', 'a', texto)
    texto_normalizado = re.sub(r'[ÉÊéê]', 'e', texto_normalizado)
    texto_normalizado = re.sub(r'[Íí]', 'i', texto_normalizado)
    texto_normalizado = re.sub(r'[ÓÔÕóôõ]', 'o', texto_normalizado)
    texto_normalizado = re.sub(r'[Úú]', 'u', texto_normalizado)
    return texto_normalizado

texto_normalizado = normalizar(texto)

# Substituir letra especificada
texto_substituido = substituir_letra(texto_normalizado, letra_antiga, letra_nova)

print(texto_substituido)
```

Fonte: Elaborado pelo autor através do chatbot ChatGPT; versão: GPT 4o. Disponível em: https://chatgpt.com/ (acesso em 20/05/2024)

- CÓDIGO EM PYTHON PARA CIFRAR UM TEXTO POR SUBSTITUIÇÃO MONOALFABÉTICA A PARTIR DE UM ALFABETO CIFRADO DADO (QUE PODE CONTER ALGARISMOS):

```
def substituir_letras(texto, alfabeto_original, alfabeto_cifrado):
    # Cria um dicionário de substituição baseado nos alfabetos fornecidos
    substituicao = str.maketrans(alfabeto_original, alfabeto_cifrado)

    # Aplica a substituição no texto
    texto_cifrado = texto.translate(substituicao)

    return texto_cifrado

# Alfabetos fornecidos (os alfabetos devem conter o mesmo número de caracteres que devem ser digitados no campo especificado sem espaços)
alfabeto_original = "abcdefghijklmnopqrstuvwxyz"
alfabeto_cifrado = "INSIRAAQUISEUALFABETOCIFRADO"
```

```
# Exemplo de uso
texto = "INSIRA SEU TEXTO AQUI."

# Normalizar o texto (removendo acentos e convertendo para minúsculas)
import re

texto_normalizado = re.sub(r'[áàâã]', 'a', texto.lower())
texto_normalizado = re.sub(r'[éê]', 'e', texto_normalizado)
texto_normalizado = re.sub(r'[í]', 'i', texto_normalizado)
texto_normalizado = re.sub(r'[óôõ]', 'o', texto_normalizado)
texto_normalizado = re.sub(r'[ú]', 'u', texto_normalizado)

# Substituir letras conforme os alfabetos fornecidos
texto_cifrado = substituir_letras(texto_normalizado, alfabeto_original,
alfabeto_cifrado)

print(texto_cifrado)
```

Fonte: Elaborado pelo autor através do chatbot ChatGPT; versão: GPT 4o. Disponível em: https://chatgpt.com/ (acesso em 20/05/2024)

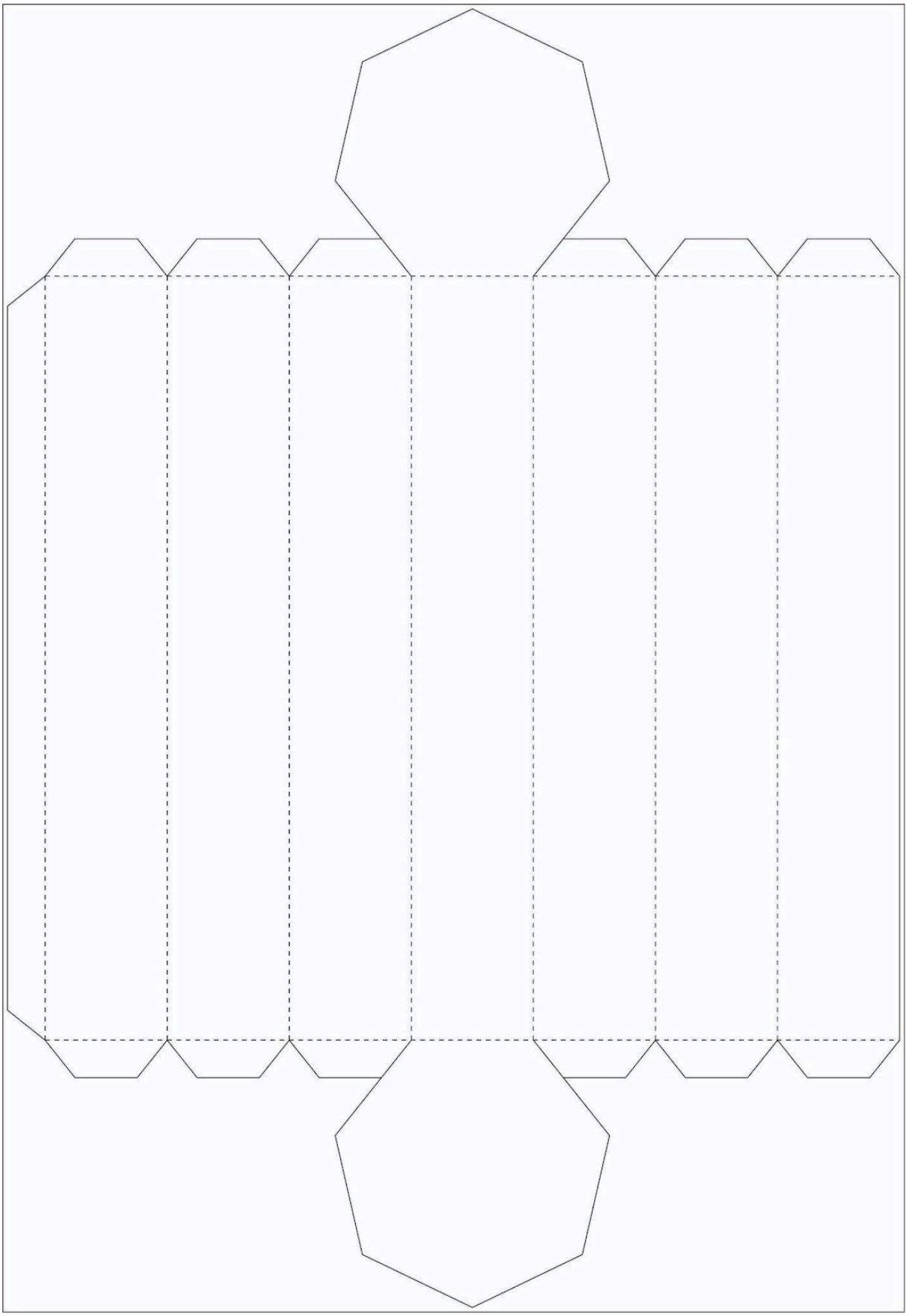
- CÓDIGO EM PYTHON PARA CIFRAR UM TEXTO POR CIFRA DE VIGENÈRE:

```
# criptografa um texto com a cifra de Vigenère

def lettre(c):
    # retorna verdadeiro se for uma letra sem acento
    car = ord(c.upper())
    return car>64 and car<91

def decalage(c,k):
    # altera uma letra para maiúscula. Outras letras não são modificadas
    car = ord(c.upper())
    if lettre(c):
        car += k
        while car>90:
            car -= 26
        while car<65:
            car += 26
        return chr(car)
    else:
        return ""
```

```
def vigenere(message,chave,crypte):
    # executa a mudança com base na chave e nos caracteres da mensagem
    n = 0
    chiffre=''
    for c in message:
        if lettre(c):
            k = ord(chave[n%len(chave)])-65
            if crypte:
                chiffre += decalage(c,k)
            else:
                chiffre += decalage(c,-k)
            n+=1
        else:
            chiffre += c
    return chiffre


# teste
chave = "INSIRA SUA CHAVE AQUI"
texte="INSIRA SEU TEXTO AQUI"
texte_code = vigenere(texte,chave,True)
print(texte_code)
texte_decode = vigenere(texte_code,chave,False)
print(texte_decode)
```

Fonte: https://www.apprendre-en-ligne.net/crypto/python/vigenere/vigenere.py (adaptado pelo autor)

- Planificação de um citale de 7 faces retangulares:



Fonte: Elaborado pelo autor

ANEXO

Anexo I: Questionário elaborado para o 9º ano do Ensino Fundamental II e para o 2º ano do Ensino Médio, como parte da avaliação das atividades práticas em sala de aula.

Dentre as alternativas das questões abaixo, selecione aquela que mais representa sua opinião em relação a seguinte afirmação:

Questão 01: As atividades contribuíram positivamente para a compreensão dos conceitos matemáticos abordados?

( ) Concordo plenamente
( ) Concordo parcialmente
( ) Não concordo nem discordo
( ) Discordo parcialmente
( ) Discordo plenamente

Questão 02: As aulas com as atividades realizadas foram mais interessantes e motivadoras do que as aulas tradicionais?

( ) Concordo plenamente
( ) Concordo parcialmente
( ) Não concordo nem discordo
( ) Discordo parcialmente
( ) Discordo plenamente

Questão 03: As atividades deixaram claras algumas possíveis aplicações dos conceitos matemáticos estudados?

( ) Concordo plenamente
( ) Concordo parcialmente
( ) Não concordo nem discordo
( ) Discordo parcialmente
( ) Discordo plenamente

Questão 04: As atividades me proporcionaram uma compreensão da importância do pensamento criativo na resolução de problemas matemáticos?

( ) Concordo plenamente
( ) Concordo parcialmente
( ) Não concordo nem discordo
( ) Discordo parcialmente
( ) Discordo plenamente

Questão 05: As atividades contribuíram para que os conteúdos estudados parecessem menos intimidadores para mim?

( ) Concordo plenamente
( ) Concordo parcialmente
( ) Não concordo nem discordo
( ) Discordo parcialmente
( ) Discordo plenamente
( ) Eu nunca achei os conteúdos intimidadores, mesmo antes das atividades.

Questão 06: As atividades práticas me encorajaram a adotar uma abordagem mais prática e experimental nos estudos de conceitos matemáticos?

( ) Concordo plenamente
( ) Concordo parcialmente
( ) Não concordo nem discordo
( ) Discordo parcialmente
( ) Discordo plenamente

Questão 07: Dentre as alternativas, selecione aquela que mais representa sua avaliação em relação às aulas com atividades práticas.

( ) Muito boa
( ) Boa
( ) Indiferente
( ) Ruim
( ) Muito ruim

Questão 08: Dentre as alternativas, selecione aquela que mais representa sua avaliação em relação ao tema central escolhido para as atividades práticas (criptografia e criptoanálise).

( ) Muito boa
( ) Boa
( ) Indiferente
( ) Ruim
( ) Muito ruim