UNIVERSIDADE FEDERAL DE SÃO CARLOS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENSINO DE CIÊNCIAS EXATAS

APLICANDO CRIPTOGRAFIA NO FORMATO DE ROTAÇÃO POR ESTAÇÕES DE APRENDIZAGEM

EDUARDO RODRIGUES LIMA

Sorocaba
2024

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CAMPUS SOROCABA

APLICANDO CRIPTOGRAFIA NO FORMATO DE ROTAÇÃO POR ESTAÇÕES DE APRENDIZAGEM

EDUARDO RODRIGUES LIMA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ensino de Ciências Exatas (PPGECE) do Centro de Ciências Exatas e Tecnologia da Universidade Federal de São Carlos - Campus Sorocaba, como exigência parcial para obtenção do título de Mestre em Ensino de Ciências Exatas.

Orientação: Prof.ª Dr.ª Silvia Maria Simões de Carvalho.

Sorocaba
2024

Lima, Eduardo Rodrigues

Aplicando criptografia no formato de rotação por estações de aprendizagem / Eduardo Rodrigues Lima -- 2024.
108f.

Dissertação (Mestrado) - Universidade Federal de São Carlos, campus Sorocaba, Sorocaba
Orientador (a): Silvia Maria Simões de Carvalho
Banca Examinadora: Luiza Amalia Pinto Cantão, Antonio Luís Venezuela
Bibliografia

1. Criptografia RSA. 2. Ensino de Matemática. 3. Rotação por estações de aprendizagem. I. Lima, Eduardo Rodrigues. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Maria Aparecida de Lourdes Mariano - CRB/8 6979

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Ensino de Ciências Exatas

Folha de Aprovação

Defesa de Dissertação de Mestrado do candidato Eduardo Rodrigues Lima, realizada em 13/12/2024.

Comissão Julgadora:

Profa. Dra. Silvia Maria Simões de Carvalho (UFSCar)

Profa. Dra. Luiza Amália Pinto Cantão (UNESP)

Prof. Dr. Antonio Luís Venezuela (UFSCar)

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Ensino de Ciências Exatas.

Agradecimentos

Agradeço primeiramente a Deus, por me conceder sabedoria e saúde ao longo desta jornada.

À minha orientadora, Prof. Silvia Carvalho, expresso minha profunda gratidão por ter aceitado o desafio de me orientar. Sua dedicação em cada discussão, revisão e sugestão de pesquisa, bem como suas valiosas indicações de leitura e apoio constante, foram fundamentais para a construção e conclusão deste trabalho. Agradeço também aos professores da UFSCar Sorocaba, que, ao longo do Mestrado, contribuíram significativamente para o meu desenvolvimento acadêmico.

Aos meus colegas do PPGECE, deixo minha sincera gratidão pelo companheirismo ao longo dessa caminhada. Juntos, enfrentamos desafios, viramos noites estudando e nos apoiamos mutuamente, especialmente nas preparações para as provas de sexta-feira, seja pela manhã ou à tarde.

Sou igualmente grato aos membros da banca avaliadora, que gentilmente aceitaram o convite para participar deste processo, oferecendo comentários e críticas construtivas essenciais para a finalização desta dissertação. Agradeço, ainda, à Universidade Federal de São Carlos – Campus Sorocaba, pela oportunidade de realizar este Mestrado profissional, que foi uma experiência transformadora.

Por fim, dedico um agradecimento especial à minha esposa, Ester, e à minha mãe, Maria Izilene, por seu apoio incondicional, por sempre acreditarem em mim e me incentivarem, especialmente nos momentos mais desafiadores.

Resumo

Este trabalho explora o uso da Criptografia em sala de aula com turmas de 8º e 9º anos do Ensino Fundamental II, em uma escola de ensino regular no interior do Estado de São Paulo. O conteúdo foi abordado em 6 horas-aula (300 minutos), partindo de conceitos teóricos já estudados, como números primos e divisibilidade, até a aplicação prática da atividade de rotação por estações de aprendizagem. Nessas atividades, os alunos enfrentaram desafios de decifração e codificação, jogos educacionais e testes individuais e em grupo. Embora o método RSA exija conhecimento sobre congruência e aritmética modular, as etapas de codificação e decodificação foram adaptadas para facilitar a compreensão dos estudantes. O processo envolveu momentos de discussão, prática colaborativa, competição e diversão, contribuindo para o desenvolvimento de novas habilidades e a retomada de conceitos matemáticos já trabalhados. O objetivo foi investigar a integração da teoria Matemática com atividades práticas, permitindo que os alunos enxergassem a Matemática além do abstrato. Com essa abordagem, tópicos frequentemente vistos apenas na teoria ganham uma nova perspectiva e se tornam mais próximos da realidade dos estudantes.

Palavras-chave: Criptografia RSA; Aritmética modular; Ensino de Matemática; Rotação por estações.

Abstract

This paper explores the use of cryptography in the classroom with 8th and 9th grade classes in a regular school in the interior of the state of São Paulo. The content was covered in 6 class hours (300 minutes), starting with theoretical concepts already studied, such as prime numbers and divisibility, and moving on to the practical application of the activity of rotating through learning stations. In these activities, students faced deciphering and coding challenges, educational games, and individual and group tests. Although the RSA method requires knowledge of congruence and modular arithmetic, the coding and decoding steps were adapted to facilitate student understanding. The process involved moments of discussion, collaborative practice, competition, and fun, contributing to the development of new skills and the review of Mathematical concepts already worked on. The objective was to investigate the integration of Mathematical theory with practical activities, allowing students to see Mathematics beyond the abstract. With this approach, topics often seen only in theory gain a new perspective and become closer to the students' reality.

Keywords: RSA cryptography; Modular arithmetic; Mathematics teaching; Station rotation.

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

A escolha pela criptografia como tema de pesquisa se deu pelo elo indissociável entre essa área e a matemática, especialmente no sistema RSA, um método atual que utiliza conceitos de aritmética para garantir a segurança das informações. Apesar da visão de muitos que enxergam o computador como uma ameaça à privacidade, a criptografia permite transformá-lo em um escudo poderoso, protegendo sistemas e dados com níveis de segurança cada vez mais sofisticados.

Ao aliar criptografia, aritmética, tecnologias e jogos educacionais, a proposta apresentada se configura como uma ferramenta educacional poderosa que, quando aplicada em sala de aula de forma assertiva, contribui positivamente na construção do conhecimento. Sua ação transcende os limites da matemática, iluminando o caminho para o progresso e o desenvolvimento de diversas habilidades essenciais para a evolução dos estudantes em todas as disciplinas.

Para que essa proposta se torne realidade, um planejamento criterioso é fundamental. A reflexão constante da prática docente, a análise minuciosa das ações durante todo o processo, a busca incessante por aprimorar procedimentos e estratégias, o aperfeiçoamento dos recursos de ensino e aprendizagem, o uso estratégico da análise do erro e a valorização da autonomia do estudante, sempre alinhados às expectativas de aprendizagem da Base Nacional Comum Curricular (BNCC), são pilares indispensáveis para o sucesso.

Motivação

- Elo indissociável entre a criptografia e a matemática, em particular o método RSA.
- Aliar criptografia, aritmética (disciplina do Mestrado) e jogos educacionais.
- Melhorar procedimentos e estratégias utilizadas no ano anterior para potencializar a metodologia de ensino e aprendizagem.

Problemática

- A falta de uma metodologia que explore a criptografia no ensino de matemática limita a capacidade dos estudantes de estabelecer conexões entre o conhecimento teórico e

a sua aplicação, comprometendo a construção de uma aprendizagem significativa. Como explorar uma metodologia alternativa de ensino aprendizagem a partir do tópico Criptografia em conjunto com os objetos de conhecimento associados a ela, como divisibilidade, múltiplos, fatoração e números primos?

- Como alcançar as metas idealizadas para as expectativas de ensino e aprendizagem, e contribuir para o desenvolvimento de habilidades essenciais para o futuro dos estudantes?

Justificativa

Explorar e abordar a criptografia com um olhar voltado para a educação matemática, a partir do uso de metodologias ativas. Assim, a criptografia será utilizada como contexto para explorar conceitos de divisibilidade, múltiplos, fatoração, números primos, e, também, para analisar sistemas criptográficos simples a partir da aplicação da metodologia de rotação por estações de aprendizagem em turmas de 8° e 9° anos do Ensino Fundamental II com o intuito de promover o ensino de matemática de forma mais atrativa, demonstrando a aplicabilidade dos conceitos matemáticos em situações reais e relevantes.

Objetivos

- Investigar o impacto da utilização de jogos de criptografia no desenvolvimento do raciocínio lógico e da resolução de problemas em alunos dos 8° e 9° ano do Ensino Fundamental II.
- Aplicar um Plano de Ensino com o objetivo de promover o desenvolvimento e a melhora de habilidades como o pensamento crítico e resolução de problemas.

Fundamentação Teórica

O tópico Criptografia não possui tantos livros escritos em nosso idioma, principalmente quando pensamos em livros voltados para: A História da Criptografia. Desta maneira, a construção de diversos trabalhos acadêmicos seguem o mesmo referencial teórico para quando se quer falar sobre o desenrolar da história: Simon Singh.

Em relação as discussões sobre os avanços Criptográficos, existe uma quantidade considerável de dissertações voltadas para a Criptografia RSA, em contrapartida tem-se poucos materiais disponíveis para Criptografia de Curvas Elípticas (ECC). Em relação as Teses, muito se fala sobre o Computador quântico, além de muitas outras pesquisas também serem voltadas para o movimento Pós-quântico.

Para ilustrar as referências utilizadas neste trabalho, seguem as principais, de acordo com o tema trabalhado:

1. História da Criptografia: Hefez (Aritmética), Singh (O livro dos códigos), British Museum (Imagens e artigos), Gomes (Dissertação - UFSCar, 2022), Carvalho (Dissertação - UFSCar, 2020) e Costa e Figueiredo (Repositório Institucional - CEDERJ).

2. Conceitos de Criptografia e Método RSA: Hefez (Aritmética), Coutinho (Números Inteiros e Criptografia RSA) e Carneiro (Criptografia e Teoria dos números).

3. Criptografia de Curvas elípticas (ECC): Okida (Dissertação - USP, 2011), Oliveira (Dissertação - UNICAMP, 2010), Pereira (Dissertação - USP, 2011), Nakamura (Dissertação - USP, 2011) e Arruda (Dissertação - UFSCar, 2014).

4. Criptografia no Ensino da Matemática: Bacich - Neto - Trevisani (Ensino híbrido), Wiggins - Mctighe (Planejamento para a Compreensão), Enkvist (O complexo ofício do professor), Ubiratan D'Ambrosio (Educação Matemática: da teoria à prática), Borba e Penteado (Informática e Educação Matemática) e Zabala (A prática educativa: como ensinar).

Vale a pena ressaltar que os repositórios de pesquisa para desenvolvimento deste trabalho foram: Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), Biblioteca Digital de Teses e Dissertações da USP e do Banco de dissertações do Programa de Pós-Graduação em Ensino de Ciências Exatas da UFSCar (PPGECE).

Metodologia

Este trabalho é uma pesquisa de natureza qualitativa (interpretativa) que possibilitará o acesso às concepções dos participantes sobre os conceitos de divisibilidade, múltiplos, fatoração e números primos na perspectiva da criptografia a partir da aplicação da metodologia de rotação por estações de aprendizagem. Além disso, para enriquecer o trabalho e trazer uma nova visão sobre o tema, serão realizadas avaliações e a coleta de dados quantitativos, discussões em grupo, criação de mapas mentais, aplicação de jogos criptográficos, entre outras atividades, mantendo-se o anonimato dos estudantes e da Escola.

O público-alvo são 96 estudantes pertencentes a duas turmas de 9º anos e uma turma de 8° ano do Ensino Fundamental de uma Instituição de Ensino Regular no interior do Estado de São Paulo. Os objetos de conhecimento associados ao tema criptografia serão trabalhados para relacionarem a teoria e a prática dos conhecimentos matemáticos desenvolvidos em sala de aula.

A forma de avaliar os conhecimentos adquiridos pelos alunos no decorrer das 6 horas-aulas (que serão utilizadas para aplicar esta proposta) será por meio da entrega de

um relatório por grupo, com questões de decodificação, decifração, função polinomial do primeiro grau, alguns acontecimentos na história da criptografia, mapa mental e as respostas entregues na atividade de rotação por estações. Além disso, no Forms (questionário) sobre o projeto aplicado, não serão coletados os nomes, mas para facilitar a análise e reflexão dos resultados dissertativos, os alunos serão denominados como: A, B, C, e assim por diante.

A jornada pela criptografia em sala de aula se inicia com uma roda de conversa para descobrir o que os estudantes sabem sobre o tema. Em seguida, uma viagem no tempo, abordando desde a antiguidade até os dias de hoje, explorando a rica história da criptografia e de seus métodos ancestrais. Posteriormente, a decodificação da escrita secreta (refletindo sobre os seus desdobramentos), além de aprender sobre as cifras de transposição e substituição. Em grupos, colocarão em prática as habilidades de descriptografia, resolvendo os desafios na atividade de rotação por estações de aprendizagem. Ao final do processo, uma avaliação em formato de quiz para verificar o conhecimento adquirido, e o Forms para receber o feedback dos alunos.

Estrutura da Dissertação

No Capítulo 1, é explorada a história da criptografia, destacando-se como uma arte milenar que tem se desenvolvido e evoluído ao longo do tempo, tornando-se cada vez mais robusta. Nesse contexto, são abordados conceitos como cifras, códigos e o sistema binário.

No Capítulo 2, são introduzidos importantes conceitos matemáticos que contribuem para a compreensão dos métodos RSA e ECC, como números primos, divisibilidade e congruência.

O Capítulo 3 foca no conceito de criptografia, com uma análise dos métodos RSA e ECC. A aplicação do método RSA é apresentada de forma mais detalhada, mostrando-se o passo a passo, desde a pré-codificação até a decodificação da mensagem: UFSCar 2024.

No Capítulo 4, discute-se a aplicação da criptografia no ensino de matemática, utilizando estratégias pedagógicas como jogos, quizzes, atividades de rotação por estações, mapas mentais e questionários. Também são apresentados os resultados de uma pesquisa realizada com os estudantes, cujas opiniões são ilustradas por meio de gráficos de setores obtidos via Forms.

Por fim, o Capítulo 5 traz as considerações finais.

Vale ressaltar que os momentos em que menciona-se aprendizagem significativa, ao decorrer do trabalho, o intuito é indicar uma aprendizagem que atenda as expectativas de aprendizagem de forma satisfatória. Sabe-se que existem vários estudos e linhas de pesquisas referentes a esse tema, mas não será possível abordá-lo nessa dissertação.

Plano de Aula

Figura 0.1: Plano de Aula - Parte 1

Professor: Eduardo Lima

Disciplina: Matemática

Tema: Criptografia

Público-alvo: 8° e 9° anos (96 estudantes)

Duração: 6 aulas (300 minutos)

Objetivos da aula:

- **Geral:** Explorar a criptografia a partir de sua relação com os conceitos matemáticos de divisibilidade, múltiplos, divisores, fatoração, potenciação e números primos, e apresentando acontecimentos importantes da história como ponto de partida para resolução de desafios de cifração e codificação.
- **Específico:** Investigar o impacto da utilização de jogos de criptografia no desenvolvimento do raciocínio lógico e da capacidade de resolução de problemas em alunos dos 8° e 9° anos do Ensino Fundamental II.

Objetos de conhecimento:

- Divisibilidade, múltiplos, fatoração, números primos e potenciação;
- Métodos de criptografia: códigos, cifras de substituição e transposição;
- Cifra de César e Criptografia RSA;
- Função polinomial do 1° grau no contexto criptográfico.

Materiais necessários (Recursos):

- Projetor multimídia e Lousa;
- Apresentação - Canva;
- Computadores e notebooks;
- Papéis e canetas para mapas mentais;
- Jogos criptográficos (desafios práticos);
- Fichas e materiais para as atividades das estações de aprendizagem.

Habilidades BNCC:

- (EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos “é múltiplo de”, “é divisor de”, “é fator de”, e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10.
- (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.
- (EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos.
- (EF08MA02) Resolver e elaborar problemas usando a relação entre potenciação e radiciação, para representar uma raiz como potência de expoente fracionário.
- (EF09MA06) Compreender as funções como relações de dependência unívoca entre duas variáveis e suas representações numérica, algébrica e gráfica e utilizar esse conceito para analisar situações que envolvam relações funcionais entre duas variáveis

Fonte: Elaborado pelo autor, 2024.

Figura 0.2: Plano de Aula - Parte 2

Procedimento Metodológico:

- Aulas 1 e 2:

- **Introdução:** uma roda de conversa inicial para levantamento dos conhecimentos prévios. Por exemplo, “O que sabemos sobre criptografia?”. Após isso, uma contextualização histórica sobre pontos importantes da evolução da criptografia.
- **Exposição teórica:** apresentação de métodos ancestrais e aplicações modernas, como o método RSA. Também uma discussão sobre o aprimoramento das Cifras ao longo dos séculos e a retomada de conceitos matemáticos relevantes para aplicação do RSA (divisibilidade, múltiplos, fatoração, potenciação, números primos e função polinomial).
- **Atividade prática:** Decodificação de mensagens secretas, a decifração da Cifra de César e da cifra que utiliza algarismos.
- **Avaliação:** aplicação de um quiz em grupo para verificação do aprendizado a partir da plataforma Kahoot.

- Aulas 3 e 4:

- **Rotação por estações de aprendizagem:** a aproposta do método é avaliar a aprendizagem dos estudantes sobre a criptografia apresentada nas duas primeiras aulas. O espaço escolhido foi a biblioteca, trabalhando-se com 5 estações de aprendizagem, sendo elas: decifração da cifra com algarismos; Cifra de César; processo criptográfico do nome completo, além de um desafio sobre função polinomial do 1° grau; construção de um mapa mental sobre tudo o que foi visto até o momento; jogo com questões sobre criptografia.
- **Jogo de criptografia:** o jogo de perseguição no labirinto sugerido na quinta estação foi construído na plataforma Wordwall e possui contagens de tempo, vidas e acertos.

- Aulas 5 e 6:

- **Forms:** é um questionário construído na plataforma Microsoft com o intuito de coletar os dados referentes a aplicação do projeto de criptografia no formato de rotação por estações de aprendizagem.
- **Quiz:** individual na plataforma Kahoot.
- **Avaliação:** entrega de um relatório com questões relacionadas as soluções encontradas em cada estação de aprendizagem.

- **Referências:** na parte histórica são as mesmas apresentadas na Dissertação. Em relação aos conceitos matemáticos, foi utilizado o livro da própria instituição que pediu anonimato. No entanto, pode-se utilizar: O livro dos códigos de Simon Singh e a plataforma Khan Academy para acompanhar o desenvolvimento das habilidades matemáticas.

Fonte: Elaborado pelo autor, 2024.

Capítulo 1

Criptografia: Uma História Milenar (Da Antiguidade ao Século XXI)

A criptografia, que etimologicamente significa *escrita secreta*, é a prática de transformar informações em mensagens indecifráveis, permitindo acesso apenas ao destinatário ou detentor da chave de descriptografia. Essa arte milenar, com origens que remontam à escrita cuneiforme mesopotâmica e aos hieróglifos egípcios, evoluiu impulsionada por aprimoramentos em métodos e técnicas, desde cifras manuais até algoritmos computacionais complexos. Como afirma Hefez (2022), a palavra *criptografia* origina-se do grego *kriptos*, que significa *oculto*, reforçando a essência dessa prática como *escrita secreta*.

Antigamente, a criptografia era utilizada para proteger mensagens confidenciais em tempos de guerra e espionagem. Hoje em dia, ela é essencial para a segurança digital, garantindo a confidencialidade de dados em transações online, protegendo informações sigilosas em bancos de dados e viabilizando a comunicação segura na internet.

Com o avanço da tecnologia, a criptografia enfrenta novos desafios, como a potencial ameaça da computação quântica (um mecanismo computacional que solucionará problemas complexos rapidamente). Os protocolos da criptografia clássica podem ser facilmente decifrados por computadores quânticos. Pesquisas contínuas buscam desenvolver métodos robustos para garantir a segurança da informação no futuro. Além disso, podemos utilizar o próprio computador quântico para codificar informações, dificultando ainda mais a tarefa de decifrá-las.

A criptografia possui uma história rica e complexa que se entrelaça com o desenvolvimento da civilização humana. Desde os primórdios da escrita até a era da computação quântica, a busca por métodos seguros de comunicação tem moldado a forma como protegemos informações confidenciais.

Por isso, o seu estudo é de extrema relevância nos dias de hoje, pois além de colaborar para a segurança individual e coletiva, abre portas para discussões sobre o papel fundamental da matemática nos sistemas de segurança da informação. Assim, números primos e a aritmética modular ganham destaque na criptografia e no mundo digitalizado.

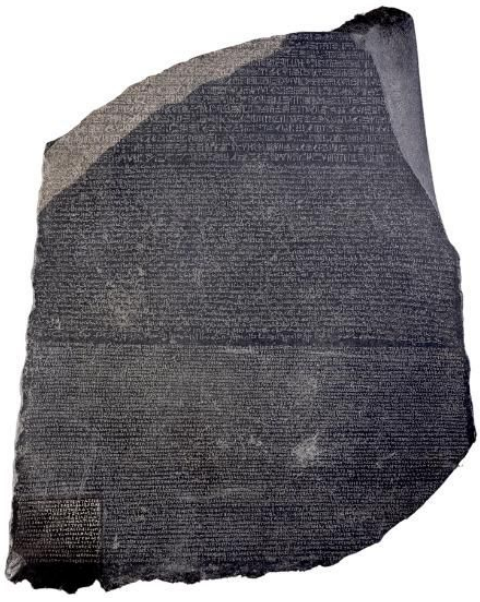
1.1 Antiguidade

No Egito Antigo, por volta de 2.000 a.C., os sacerdotes detinham o conhecimento da escrita hierática, um sistema intrincado de símbolos e ideogramas que ilustravam textos religiosos e governamentais. Para o povo comum, que utilizava a escrita demótica mais simples e acessível, esses textos hieráticos eram indecifráveis, servindo como uma forma natural de criptografia para proteger segredos e conhecimentos ancestrais.

Ao desvendar a história da matemática no Egito antigo, os pesquisadores até o século XIX enfrentaram duas grandes dificuldades, como destacam Boyer e Merzbach (2019, p. 29): "a inabilidade de ler os materiais-fonte e a escassez desses materiais". Essa dificuldade de decifrar as escritas e a falta de documentos preservados impediram um maior entendimento da matemática praticada pelos egípcios. Além disso, a escrita hieroglífica passou por transformações, desde formas puramente ideográficas até hierática mais fluida e, finalmente, a demótica, ainda mais rápida.

Na Figura 1.1 temos a Pedra de Roseta, um artefato histórico fundamental para a compreensão da escrita hieroglífica egípcia. Para ser amplamente compreendida, a pedra contém um decreto real gravado em três idiomas: hieróglifos egípcios (adequados para um decreto sacerdotal), demótico (que significa *língua do povo*) e grego antigo.

Figura 1.1: A Pedra de Roseta, el-Rashid, Egito, 196 a.C.

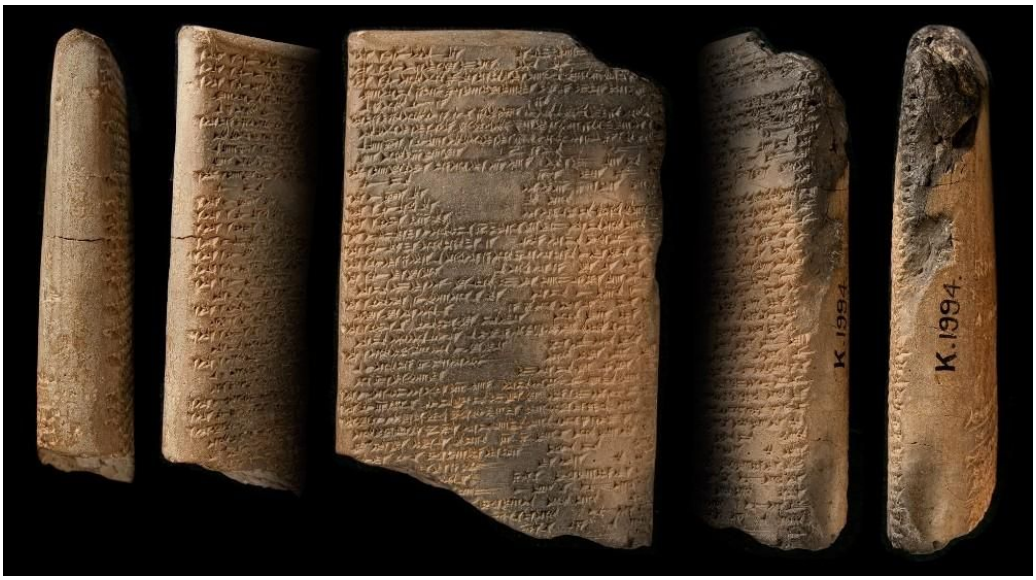


Fonte: BRITISH MUSEUM (Timeline of ancient Egypt).

Na Mesopotâmia, no mesmo período, a escrita cuneiforme, esculpida em placas de argila com estiletes afiados, também funcionava como um código sigiloso. Essa escrita complexa, composta por símbolos em forma de cunha, era dominada por escribas e sacerdotes, tornando-a inacessível para a grande maioria da população. Essa exclusividade da escrita cuneiforme permitia aos governantes e elites controlar o acesso à informação e consolidar seu poder.

Pode-se observar na Figura 1.2, tabuletas cuneiformes que foram usadas para registrar tudo, desde a administração cotidiana até a Ciência e a Literatura.

Figura 1.2: Fragmento de tábua de argila com inscrição em cuneiforme, escrita para a biblioteca de Assurbanipal. Século VII a.C.



Fonte: BRERETON. British Museum. 2018.

O último grande rei da Assíria, Assurbanipal, que governou entre 669 e 631 a.C., foi responsável por construir a Grande Biblioteca de Nínive. Ele nutria um fascínio ímpar pelos livros. Sua biblioteca, a maior do mundo antigo, reunia exemplares de diversas áreas do conhecimento, indo muito além do mero divertimento. Através desses textos, Assurbanipal buscava não só sabedoria, mas também a conexão com o divino e a compreensão dos mistérios do futuro. Como BRERETON (2018) enfatiza, a coleção real abrangia uma ampla gama de temas, incluindo presságios divinatórios obtidos por meio de sacrifícios, estudos do céu e do mundo terreno, rituais e calendários precisos, hinos e orações elevadas, além de tratados de magia e medicina.

Além disso, Gareth Brereton (2018) menciona que o rei Assurbanipal também contava com um *correio real*, mensageiros que eram enviados para transmitir mensagens, decretos reais, notícias do front de batalha, relatórios de impostos etc., além de serem uma rede de comunicações confiável e competente. Eles viajavam por estradas reais que foram construídas e conectadas com o objetivo de agilizar o processo de envio e recebimento de informações, ao longo da estrada eles se comunicavam por meio de sinais de fumaça, sinais visuais e mensageiros a cavalo.

Embora os mensageiros enfrentassem condições climáticas adversas, bandidos, animais selvagens, e outros obstáculos, conseguiam cumprir a missão que lhe eram incumbidos. Gareth assegura que eles eram homens altamente treinados e experientes, que dedicavam suas vidas ao serviço do rei. Por isso, em apenas alguns dias, as mensagens saiam da capital e chegavam aos confins do império, e vice-versa.

Na Figura 1.3, pode-se ver uma carta e envelope de argila, datado do século VIII a.C.,

que era transportado por mensageiros do correio real, que são homens de maior confiança do rei. Vale a pena ressaltar que as cartas eram seladas por anéis de sinete dourado gravado com a imagem do rei matando um leão feroz.

Figura 1.3: Carta e envelope de argila do século VIII a.C

Fonte: BRERETON. British Museum. 2018.

No século V a.C., o Bastão de Licurgo (Figura 1.4), se destacava como um artefato histórico crucial para a comunicação entre as cidades da Esparta Antiga, especialmente durante as Guerras Médicas e Guerra do Peloponeso. Sua função primordial era garantir a segurança das informações trocadas entre os líderes militares, assegurando a confidencialidade de mensagens estratégicas. Como afirma Gomes (2022, p. 15): "o Bastão de Licurgo, consiste em uma cifra de transposição, que era utilizado para transmitir mensagens confidenciais."

Figura 1.4: Bastão de Licurgo.

Fonte: MEDEIROS, Fávio. 2015.

Outra Cifra desenvolvida na Antiguidade, entre 200 a.C. e 118 a.C., é a de Políbio, que utilizava cinco letras como base de codificação de mensagens e possuía uma tabela pré-definida de fácil memorização, possibilitando uma comunicação segura até mesmo em longas distâncias ou mau tempo a partir de sinais luminosos emitidos por tochas.

Ao longo da história, a criptografia se revelou uma ferramenta poderosa e versátil, transcendendo os limites da guerra e se infiltrando em diversos âmbitos da sociedade.

Sua trajetória evolutiva, marcada por três fases distintas, demonstra como essa técnica inovadora moldou a forma como as informações são protegidas e transmitidas. Conforme destaca Gomes (2022, p. 16): "o seu desenvolvimento é marcado por três fases: artesanal, mecânica e digital. A primeira fase , registra a utilização inicial da criptografia em paralelo com o desenvolvimento da escrita...".

O imperador Júlio César, por volta de 50 a.C., também desenvolveu um código de troca de mensagens, que ficou conhecido como *Cifra de César*. Ele utilizava esse método para enviar mensagens secretas aos seus generais e, assim, conseguia operar ou remanejar de forma mais eficiente os seus exércitos, o que proporcionou a vitória em inúmeras batalhas. "Nesse método as letras eram substituídas pela letra que estava a três posições à direita, formando um texto sem sentido."(CARVALHO, 2020, p. 17).

A cifra de substituição monoalfabética de César, embora simples na sua concepção, foi uma ferramenta inestimável para a comunicação secreta em tempos de baixa alfabetização. Sua relevância reside não apenas na sua efetividade prática, mas também no papel que desempenhou como precursor dos métodos modernos de criptografia, abrindo caminho para um mundo onde a segurança da informação se tornou cada vez mais crucial.

Observe o uso da Cifra de César para cifrar a sigla da UFSCar (Universidade Federal de São Carlos). Note que, na Tabela 1.1, a primeira linha representa o nosso alfabeto e, a segunda linha, o alfabeto deslocado três casas à direita. De acordo com Hefez (2022, p. 212): "esse tipo de sistema criptográfico é chamado de cifra por *substituição simples*."

Tabela 1.1: *Cifra de César*

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

Fonte: Elaborado pelo autor, 2024.

A utilização da Cifra de César para criptografar a sigla **UFSCar** resulta em **XIVFDU**. De fato, essa criptografia simples torna a mensagem mais difícil de ser decifrada por quem não tem a chave (deslocamento de 3 posições). Além da Cifra de César, existem outros métodos que podem aumentar a segurança da criptografia, como a transposição de letras ou a inclusão de símbolos.

Singh (2001, p. 27) afirma que, "por convenção, na criptografia escreve-se o alfabeto correto em minúsculas e o alfabeto criptografo em maiúsculas."Essa distinção visual facilita a identificação dos elementos e a compreensão das operações criptográficas. Assim, a mensagem original (texto correto) é grafada em minúsculas, enquanto a mensagem cifrada assume letras maiúsculas.

Das brumas da Antiguidade, onde segredos e mensagens cifradas eram sussurrados, emergiu a Idade Média (476 d.C. - 1453 d.C.), um período marcado por desafios, avanços e novas aplicações da criptografia.

1.2 Idade Média e Renascimento

Na Idade Média, grande parte do conhecimento da época, incluindo avanços em criptografia e áreas afins, foi sufocada pela crença de que se tratava de magia proibida ou bruxaria. Essa perseguição, especialmente na primeira metade do período, teve um impacto devastador no progresso científico e intelectual.

Movidos por dogmas religiosos, tribunais religiosos e civis condenavam mensagens codificadas ou misteriosas como práticas malignas e profanas. Essa visão distorcida do conhecimento criptográfico era usada como ferramenta para incriminar indivíduos e silenciar vozes dissidentes.

As consequências dessa repressão foram nefastas. O desenvolvimento da criptografia e de outras áreas do saber foi severamente prejudicada, atrasando o progresso científico por séculos. A busca por conhecimento se tornou um ato perigoso, e muitos estudiosos foram silenciados ou perseguidos por suas ideias.

Ainda que Carvalho (2020, p. 18) mencione a criptografia como uma "brincadeira"entre os monges medievais, essa prática lúdica tornou-se uma ferramenta essencial para segurança da informação, principalmente no aperfeiçoamento de técnicas de codificação, possibilitando um ponto de partida para as próximas gerações. Assim, a partir dos métodos rudimentares da Antiguidade, a Idade Média promoveu as bases para o desenvolvimento da criptografia em séculos posteriores.

O Antigo Testamento da Bíblia apresenta exemplos intrigantes e deliberados de criptografia, desafiando os monges com trechos codificados em *atbash*, um método de cifra de substituição hebraica. Segundo Singh (2001, p. 43), "o atbash funciona substituindo cada letra por outra que esteja à mesma distância do final do alfabeto, quanto a letra original está do início". Um exemplo notável se encontra em Jeremias 25:26 e 51:41, onde a palavra "Babel"é substituída por "Sheshach".

Nos séculos IX e X, os árabes não se limitaram apenas ao aprimoramento de técnicas matemáticas e astronômicas. Eles também tiveram sua contribuição com a criação da criptoanálise, a arte de desvendar códigos secretos. "Esse método utilizava a análise de frequências para "quebrar" códigos monoalfabéticos, onde cada letra do texto original é substituída por uma única letra no alfabeto cifrado."(GOMES, 2022, p. 17).

Essa mesma curiosidade e engenhosidade se manifestaram no fascínio que os hieróglifos egípcios exerciam sobre os viajantes árabes medievais. Eles buscavam decifrar esses símbolos antigos para desvendar os segredos da ciência e da magia. Alguns árabes tentaram usar os hieróglifos como um código para o alfabeto árabe, enquanto outros buscaram a ajuda de falantes coptas para entender os textos antigos.

Na Figura 1.5, pode-se observar uma parte de um manuscrito, onde se tem uma tentativa árabe de decodificar hieróglifos. Embora os manuscritos originais árabes sobre hieróglifos sejam raros, as cópias e traduções europeias demonstram a popularidade desse interesse.

Figura 1.5: Livro: *A escrita do templo, linguagem de Enoque - que a paz esteja com ele*, 1776.

Fonte: BRITISH MUSEUM Board, Add MS 23420/1.

No século XVI, a história registra a primeira vítima famosa por causa da segurança de suas mensagens criptografadas: Mary Stuart da Escócia. As mensagens da rainha escocesa foram decifradas por meio do método de criptoanálise, permitindo que as cartas fossem usadas como provas de conspiração contra sua prima, Elizabeth I da Inglaterra. (SINGH, 2001, p. 17-19)

A Mary Stuart (1542 - 1587) aprendeu a criptografar com a sua mãe, Marie de Guise. De acordo com Giannini (2023), "os documentos estavam totalmente cifrados, inclusive a data e a assinatura". Segundo ele, para o trio de decifradores: George Lasry, Norbert Biermann e Satoshi Tomokiyo, conseguirem decifrar o código de 200 símbolos, foram necessários misturarem técnicas analógicas e algoritmos digitais, além de análise linguística.

Vale ressaltar que a decifração das cartas de Mary Stuart teve um impacto crucial em seu destino. As mensagens codificadas, que revelavam seus planos e conspirações contra a rainha Elizabeth I da Inglaterra, foram utilizadas como provas irrefutáveis em seu julgamento. Assim, a revelação de seus segredos selou seu destino e culminou em sua execução em 1587. É possível ver algumas de suas cartas criptografadas na Figura 1.6.

Figura 1.6: Cartas de Mary Stuart criptografadas

Fonte: GIANNINI. Bibliothèque nationale de France, 2023.

Até este momento, percebe-se o uso das cifras por transposição e substituição. Para Singh (2001, p. 26), a diferença entre elas é que "a transposição faz com que cada letra mantenha sua identidade, mas muda posição, enquanto a substituição faz com que as letras mudem de identidade, retendo a posição."Desta forma, enquanto uma reorganiza a ordem dos caracteres, a outra realiza a troca.

No final da Idade média, em meados do século XIV, a Europa presenciava o surgimento do Renascimento, um período marcado por um profundo interesse na cultura clássica, no humanismo e na valorização da razão. Nesse cenário de transformações, Leon Battista Alberti, revolucionou a área da criptografia com a criação da Cifra de Alberti, um método inovador de codificação que utilizava dois discos concêntricos para substituir letras de forma polialfabética.

Segundo Hefez (2022, p. 213), "tratava-se do uso de um artefato, chamado de *disco de Alberti*, consistindo em dois discos concêntricos de diâmetros distintos, presos por um pino central, o menor sobre o maior, podendo o disco menor girar."

Além dos avanços científicos mencionados anteriormente, outro marco significativo no âmbito da criptografia foi a publicação do livro *Poligrafia* em 1518 por Johannes Trithemius. Essa obra se destaca por introduzir um sistema criptográfico inovador e de grande impacto: a Tabula Recta. Ela consistia em uma tabela com o mesmo número de linhas e colunas, contendo o alfabeto na ordem comum na primeira linha. Nas linhas subsequentes, realizava-se uma permutação circular da linha anterior. Essa simplicidade e flexibilidade tornaram a Tabula Recta um método popular e eficiente para criptografar

mensagens.

Para ilustrar o seu funcionamento, observe a Tabela 1.2:

Tabela 1.2: Tabula Recta

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

Fonte: HEFEZ, Abramo. 2022, p. 220.

Consoante Hefez (2022, p. 214):

> A primeira letra da mensagem cifrada é transformada na letra correspondente da segunda linha, a segunda letra é transformada na letra correspondente da terceira linha e, assim, sucessivamente até esgotarem-se todas as linhas, quando se volta para a segunda linha novamente. Assim, por exemplo, a frase *mensagem para o rei* é transformada em *NGQWFMLU YKCM B FTY*.

O desejo de manter a privacidade e a segurança das comunicações é intrínseco à humanidade. Desde os primórdios da civilização, buscamos maneiras de proteger mensagens confidenciais. Como bem destacam Costa e Figueiredo (2010, p. 44), "surge também o desejo de interceptar as mensagens e decifrá-las, desde motivos militares, religiosos e políticos, até mesmo para motivos de curiosidade."

Em vista disso, surge a criptoanálise como ferramenta essencial para enfraquecimento da segurança da informação. A criptografia, como define a dupla de autores, "é a área do conhecimento encarregada de produzir técnicas que permitam a transmissão secreta de mensagens."Por outro lado, a criptoanálise, "cuida da elaboração de técnicas para decifrar mensagens criptografadas."

A Idade Média, envolta em dogmas religiosos e com perseguição ao conhecimento, rejeitou a criptografia e a criptoanálise, sufocando o progresso em diversos campos, atrasando o desenvolvimento de diversas áreas. Contudo, o Renascimento trouxe um sopro de vida renovado, despertou o interesse pela ciência e pela razão, o que possibilitou o resgate do conhecimento criptográfico. Assim, vários estudiosos passaram a se dedicar à análise de textos antigos, desvendando segredos e técnicas que haviam sido esquecidas. Aprimorando-as e buscando o desenvolvimento de técnicas mais sofisticadas, impulsionaram o progresso da criptografia.

1.3 Idades Moderna e Contemporânea

Embora as cifras monoalfabéticas apresentassem limitações inerentes à segurança, a busca por métodos melhores se intensificou com o surgimento do ataque de análise de frequência. "Coube nesse momento aos criptógrafos desenvolverem uma nova cifra que se prove imune ao ataque de análise de frequência."(LOUREIRO, 2014, p. 5).

A análise de frequência é um método em criptografia que se baseia na quantidade de vezes que cada letra do alfabeto tende a aparecer em um texto. Na língua portuguesa, por exemplo, as vogais geralmente são mais frequentes que as consoantes, e a letra "a"é a vogal mais comum. Ao analisar esses padrões de frequência, é possível realizar a criptoanálise, decifrando mensagens cifradas.

Na Tabela 1.3, é possível verificar os percentuais de ocorrência de cada letra da Língua Portuguesa.

Tabela 1.3: Análise de Frequência na Língua Portuguesa.

ALFABETO	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
FREQUÊNCIA (%)	14,63	1,40	3,88	4,99	12,57	1,02	1,30	1,28	6,18	0,40	0,02	2,78	4,74	5,50	10,73	2,52	1,20	6,53	7,81	4,34	4,63	1,67	0,01	0,21	0,01	0,47

Fonte: HEFEZ, Abramo. 2022, p. 213.

Dessa forma, o ataque de análise de frequência ocorre da seguinte maneira: identifica o percentual de ocorrência de cada letra do alfabeto, e, a partir disso, compara-se as frequências das letras cifradas com as frequências das letras na língua portuguesa para tentar decifrar o texto. Também é importante ressaltar que este método não é infalível, pois a frequência das letras varia de acordo com o tamanho do texto e com o conteúdo da mensagem. Além disso, a análise de frequência pode ser ineficaz contra textos curtos ou com tabelas de substituição complexas.

Nesse cenário, ainda precisasse levar em consideração as línguas utilizadas, pois de acordo com o idioma têm-se frequências de ocorrências diferentes. Essa análise coincide com a perspectiva de Hefez, que destaca que a principal fraqueza dos sistemas criptográficos por substituição simples reside na frequência distinta das letras em cada idioma, além da existência de regras rígidas de combinação, como a combinação obrigatória de q com u em português.

Em meio à crescente busca por comunicação segura, a cifra de Vigènere, criada por Blaise Vigenère no século XVI, representou um marco na história da criptografia. Ao introduzir o uso de múltiplos alfabetos para codificação, a cifra elevou significativamente o seu nível de segurança, dificultando consideravelmente a decifração de mensagens confidenciais. No entanto, através de técnicas inovadoras e de um profundo conhecimento matemático, Babbage conseguiu decifrar a cifra de Vigenère, que na época era considerada invencível.

Essa façanha demonstra a genialidade de Babbage e seu papel crucial no desenvolvimento da criptoanálise. Como bem destaca Bruno (2017), "a criptografia e a criptoanálise são dois lados de uma batalha, que é travada ao longo dos séculos". As descobertas de Babbage reforçam essa ideia, evidenciando a corrida armamentista entre a necessidade de segurança e a busca por métodos de decifração cada vez mais sofisticados.

Embora a Tabula Recta (século XV) e a Cifra de Vigenère (século XVI) apresentem conceitos intimamente relacionados, não são conceitos idênticos. Ambas se baseiam em tabelas quadradas e na técnica de substituição polialfabética, utilizando uma chave para determinar o deslocamento de cada letra da mensagem. No entanto, a Tabula Recta possui um leque de aplicações mais amplo que a Cifra de Vigenère, que se restringe à criptografia. A Tabula Recta, em sua forma simples, pode ser utilizada para criar tabelas de multiplicação ou para traduzir mensagens entre diferentes alfabetos.

Samuel Morse (1791-1892), um americano visionário, legou ao mundo o Código Morse, um sistema de comunicação inovador que utiliza pontos e traços para representar letras e símbolos. Esta invenção revolucionária, que se baseava na simplicidade e na eficiência, desempenhou um papel crucial na comunicação durante o século XIX e início do XX, impulsionando o comércio, a diplomacia, o jornalismo e a navegação marítima.

De acordo com Costa e Figueiredo (2010, p. 29), o Código Morse "desempenhou um papel fundamental na transmissão de mensagens codificadas até a Segunda Guerra Mundial."A Tabela 1.4, com sua correspondência engenhosa entre pontos, traços e caracteres, ilustra a elegância e a praticidade dessa ferramenta.

Tabela 1.4: Código Morse

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: GUITARRARA, Paloma. 2023.

Inicialmente, o Código Morse foi fundamental para a comunicação à distância, im-

pulsionado pelo telégrafo. Posteriormente, seu uso se expandiu para o envio de alertas e mensagens cifradas, garantindo a segurança e a confidencialidade da informação. Embora sua popularidade tenha diminuído com o tempo, o Código Morse ainda encontra utilidade em situações específicas, como sinalizar um pedido de socorro através do SOS (... _ _ _ ...).

É importante ressaltar que, embora tenha sido extremamente relevante em sua época, o Código Morse não reinou supremo de forma absoluta. A partir da Segunda Guerra Mundial, sua importância começou a declinar gradativamente, impulsionada pelo surgimento de novas tecnologias como o telefone, o rádio e, posteriormente, as telecomunicações digitais.

A cifra ADFGVX, também conhecida como supercifra, se destaca como um método de criptografia robusto, empregando diversas técnicas criptográficas em conjunto para blindar mensagens confidenciais. Sua fama se consolidou durante a Primeira Guerra Mundial (1914 - 1918), quando os alemães a utilizaram combinando dois métodos: transposição e substituição. Apesar de sua robustez, a cifra sucumbiu após apenas três meses de uso, revelando seus segredos.

O funcionamento da ADFGVX se baseia em uma tabela gerada aleatoriamente. Essa tabela é construída com seis letras dispostas na horizontal e na vertical (ADFGVX), preenchendo as demais células com as 26 letras do alfabeto e os 10 dígitos, todos embaralhados aleatoriamente. Essa complexa estrutura a torna mais resistente a ataques em comparação com as cifras tradicionais. A Tabela 1.5 serve como base para a substituição das letras na mensagem original, garantindo um alto nível de segurança.

Tabela 1.5: Cifra ADFGVX

	A	**D**	**F**	**G**	**V**	**X**
A	k	1	g	y	5	f
D	l	a	4	h	2	m
F	s	3	z	q	7	t
G	v	j	b	9	i	e
V	r	8	p	w	0	u
X	c	x	6	o	d	n

Fonte: SCHANKOSKI, 2015, p. 15.

Agora, para ilustrar o uso Cifra ADFGVX, observe as etapas de cifragem da sigla PPGECE (Programa de Pós-Graduação em Ensino de Ciências Exatas). A Tabela 1.5 servirá como guia para transformá-la em uma mensagem codificada. Cada letra da sigla será substituída por uma combinação única de letras da tabela, formulando um código indecifrável para olhos desatentos. A transformação se dará por: **P** = FV, **P** = FV, **G** = FA, **E** = XG, **C** = AX e **E** = XG. Para tornar o código ainda mais impenetrável, utiliza-se uma chave secreta como, por exemplo, a palavra “cume”.

Seguindo a ordem das letras codificadas e utilizando a chave secreta para embaralhar a sequência, obtêm-se a Tabela 1.6. Essa tabela será a fortificação que protegerá a mensagem

codificada, mas note que a escolha de uma palavra secreta mais complexa, contendo letras maiúsculas, minúsculas, números e símbolos, seria muito mais eficaz para aumentar o nível de segurança do código do que a palavra escolhida no exemplo.

Tabela 1.6: Cifragem da sigla PPGECE com base na Cifra ADFGVX

C	U	M	E
F	V	F	V
F	A	X	G
A	X	X	G

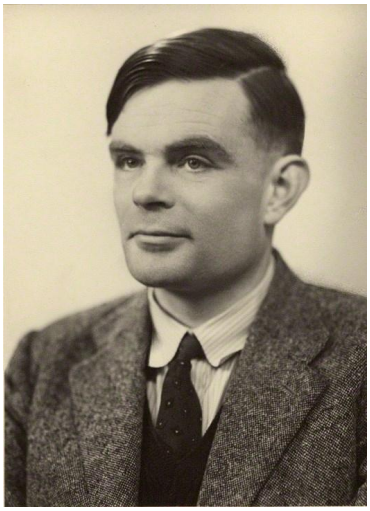
Fonte: Elaborado pelo autor, 2024.

Conforme Schankoski (2015, p. 15), a mensagem final codificada, no caso CUMEFVFV-FAXGAXXG, seria transmitida via rádio em código Morse. Essa escolha estratégica garante a segurança da mensagem, pois as letras ADFGVX, utilizadas na tabela de codificação, apresentam códigos Morse com diferenças significativas. Essa característica dificulta a quebra da cifra por meio de análise de frequências, tornando-a mais resistente a ataques em comparação com cifras tradicionais.

No cerne de todo método criptográfico reside a utilização de chave(s) que permitem ao emissor e ao receptor desvendar a mensagem codificada. Essa chave, crucial para a segurança da comunicação, precisa ser compartilhada de forma sigilosa entre ambas as partes, evitando a interceptação e a quebra da cifra por terceiros.

Um exemplo histórico do uso de chaves em criptografia é a famosa máquina Enigma, utilizada pelos alemães durante a Segunda Guerra Mundial (1939 - 1945). Apesar da constante evolução do sistema, combinando mais rotores e ligações elétricas, os aliados, liderados por mentes brilhantes como Alan Turing (Figura 1.7), conseguiram decifrar a Enigma, contribuindo significativamente para a vitória na guerra.

Figura 1.7: Alan Turing (1912 - 1954)



Fonte: National Portrait Gallery, 1951.

Hefez (2022, p. 215) destaca que a Enigma, inventada pelo engenheiro alemão Arthur Scherbius no início do século XX e inspirada no disco de Alberti, era uma máquina eletromecânica. Sua quebra teve um impacto global, alterando o panorama da criptografia e da segurança da informação.

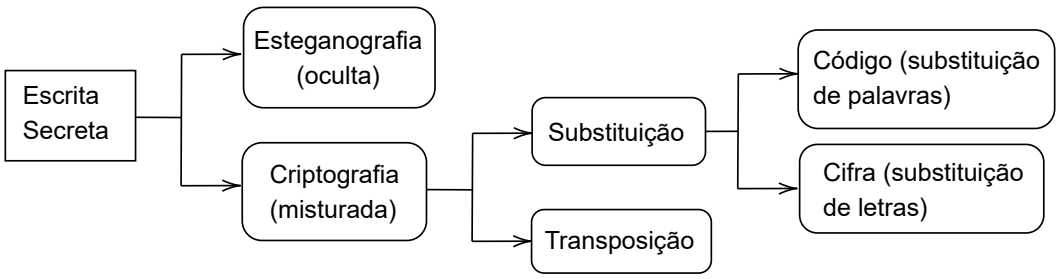
O funcionamento da Enigma se baseava na embaralhação das letras da mensagem original por meio de um circuito ajustado por uma chave trocada diariamente. Esse sistema, que demandou grande esforço dos britânicos para ser quebrado, representava o modelo simétrico de criptografia, onde a mesma chave é utilizada para cifrar e decifrar.

Embora os termos *código* e *cifra* sejam frequentemente utilizados como sinônimos, na verdade, possuem distinções importantes. Segundo Singh (2001, p. 47), "um código substitui palavras ou frases inteiras, enquanto uma cifra substitui letras individuais". Ou seja, *codificar* envolve ocultar a mensagem usando um sistema de substituição de palavras ou frases, enquanto *cifrar* consiste em embaralhar a mensagem usando técnicas de substituição de letras. Além disso, quando se quer mascarar ou esconder uma mensagem dentro de outra, usa-se a esteganografia.

Analogamente, os termos *decifrar* e *decodificar* se aplicam, respectivamente, à tradução de mensagens cifradas e codificadas. *Decifrar* significa desvendar o significado de uma mensagem embaralhada por meio de uma cifra, enquanto *decodificar* consiste em converter uma mensagem oculta por meio de um código em sua forma original.

A Figura 1.8 apresenta um esquema resumido sobre as definições abordadas:

Figura 1.8: Esteganografia x Criptografia



Fonte: SINGH, Simon (2001, p.47).

À primeira vista, os códigos podem parecer mais seguros do que as cifras, pois as palavras não se submetem à análise de frequências da mesma forma que as letras, além da vasta quantidade de palavras distintas em cada idioma. No entanto, para alcançar um nível de segurança adequado com um código, é necessário um livro-código extenso, o que torna sua viabilidade complexa. A perda desse livro-código comprometeria todo o trabalho de criptografia. Em contrapartida, as cifras exigem apenas a troca da chave em caso de comprometimento, o que simplifica a recuperação da segurança.

Vale ressaltar que a era da criptografia simétrica estava chegando ao fim. Novos métodos, como a criptografia assimétrica, surgiam com o objetivo de superar as limitações do sistema simétrico em relação à distribuição segura de chaves.

1.4 Era digital

Ao longo dos tempos, a criptografia se reinventou através de diversos métodos desenvolvidos, empregando técnicas de cifração cada vez mais sofisticadas para proteger mensagens e garantir a segurança da comunicação. Desde mensageiros, cartas e espiões até telégrafos e telefones, a busca pela transmissão de informações confidenciais de forma segura sempre foi um desafio. A chegada dos computadores marcou um ponto de virada de chave para o mundo, revolucionando os conceitos sobre segurança da informação e abrindo as portas para novos desafios e oportunidades na área da criptografia.

Para Singh (2001, p. 319):

> O sucesso da Era da Informação depende da capacidade de proteger essas informações enquanto elas fluem ao redor do mundo e isto depende do poder da criptografia. A cifragem pode ser vista como a fonte das chaves e trancas da Era da Informação. Durante dois mil anos ela foi importante apenas para o governo e os militares, mas hoje ela também tem um papel a desempenhar na facilidade dos negócios e, no futuro, pessoas comuns dependerão da criptografia para proteger sua privacidade.

Com o poder dos computadores, os criptógrafos embarcaram em uma nova jornada: a busca por cifras mais complexas e resistentes à quebra. A capacidade de realizar testes e simulações com rapidez inigualável, tornou essa missão ainda mais desafiadora, exigindo dos especialistas, criatividade e engenhosidade para criar códigos que pudessem resistir aos ataques dos computadores mais poderosos.

Os computadores operam na linguagem binária, um sistema de representação de informações que utiliza apenas dois dígitos: 0 e 1. Para que os computadores pudessem processar qualquer tipo de informação, era necessário convertê-la para esse sistema. Essa mudança de base, do decimal para o binário, foi crucial para o avanço da tecnologia e da comunicação digital. Além disso, como confirma Hefez (2022, p. 216), "foi necessário uma uniformização nos procedimentos". Assim, nasceu o ASCII (American Standard Code for Information), que é "um Código Padrão Americano para o Intercâmbio de Informação".

Por exemplo, o ano de 2024 é representado no sistema binário como: 11111101000. Para chegar nesse resultado, precisa-se realizar divisões sucessivas dos quocientes obtidos pela divisão por 2 até o momento em que a divisão não é mais possível de ser feita, conforme as etapas vistas a seguir:

(i) Inicia-se dividindo 2024 por 2, obtendo-se: quociente igual a 1012 e resto zero. Assim, registra-se o resto 0 como primeiro dígito binário, pois não sobrou nada da divisão.

(ii) 1012 dividido por 2: quociente igual a 506 e resto 0.

(iii) 506 dividido por 2: quociente igual a 253 e resto 0.

(iv) 253 dividido por 2: quociente igual a 126 e resto 1.

(v) 126 dividido por 2: quociente igual a 63 e resto 0.

(vi) 63 dividido por 2: quociente igual a 31 e resto 1.

(vii) 31 dividido por 2: quociente igual a 15 e resto 1.

(viii) 15 dividido por 2: quociente igual a 7 e resto 1.

(ix) 7 dividido por 2: quociente igual a 3 e resto 1.

(x) 3 dividido por 2: quociente igual a 1 e resto 1.

(xi) 1 dividido por 2: quociente igual a 0 e resto 1.

Agora, juntando os restos das divisões sucessivas na ordem inversa, obtêm-se a base binária: 11111101000. Esse processo também é chamado de mudança de base, então realizando a alteração da base decimal para binária, adquire-se: $0 \times 2^0 + 0 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 + 0 \times 2^4 + 1 \times 2^5 + 1 \times 2^6 + 1 \times 2^7 + 1 \times 2^8 + 1 \times 2^9 + 1 \times 2^{10}$.

No Brasil em anos de eleição são utilizadas as urnas eletrônicas para apurar a quantidade de votos dos cidadãos em seus respectivos candidatos. Os eleitores também podem se abster, votar nulo, se justificar em casos em que esteja ausente do seu domicílio eleitoral no dia e horário da eleição (das 8 às 17 horas) em outra localidade, nos casos de falta não justificada paga-se uma multa, não votando em três eleições consecutivas é cancelada a inscrição do eleitor. Além disso, existem fiscais e policiamento para a segurança do processo eleitoral.

Em relação ao funcionamento das urnas eletrônicas, todos os anos parte da população questiona sobre a sua segurança e veracidade dos resultados apresentados. Mas seria possível fraudá-la? De acordo com o TRIBUNAL REGIONAL ELEITORAL - TRE (2024), "desde as Eleições 1996, quando as urnas eletrônicas foram usadas pela primeira vez, nunca foi comprovado nenhum caso de fraude."De fato, um das principais fontes de segurança é a não conexão das urnas com a internet, impossibilitando que o equipamento adultere a quantidade de votos, favorecendo um ou outro candidato.

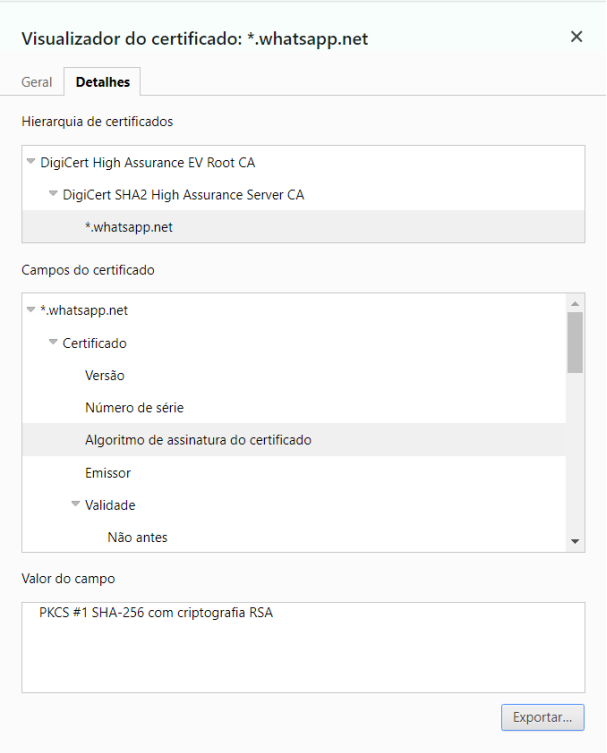
Vale evidenciar que o mecanismo de segurança das urnas eletrônicas é a criptografia. Em conformidade com o TRIBUNAL SUPERIOR ELEITORAL - TSE (2024), são utilizados "algoritmos proprietários de cifração simétrica e assimétrica, de conhecimento exclusivo do TSE". Aliás, eles acrescentam que "o boletim de urna é criptografado de forma segmentada, assinado digitalmente e transmitido."Assim, o sistema eleitoral utiliza-se de programas computacionais que garantem sua legitimidade, não permitindo fraudes em nenhum momento do processo de votação.

Nos dias de hoje, com a ascensão da internet, desenvolvimento de redes sociais e a alta do uso de aplicativos, o *WhatsApp* vem se destacando como uma excelente ferramenta de compartilhamento de mensagens. Ele é um dos aplicativos de mensagens instantâneas conectados à internet mais utilizados no país. Iniciou-se como um simples aplicativo de

troca de SMS (serviço de mensagem curta), agora possibilita o envio e recebimento de diversos tipos de mensagens, como textos, fotos, vídeos, links, documentos, mensagens de voz, assim como a localização em tempo real. Além disto, em uma atualização recente, disponibilizaram as mensagens e fotos temporárias, como também a edição de mensagens enviadas.

Na Figura 1.9, a tela do WhatsApp exibe uma mensagem informativa sobre a presença da criptografia como medida de segurança para os usuários.

Figura 1.9: Criptografia no WhatsApp



Fonte: WhatsApp.

O conglomerado Meta Platforms Inc., liderado por Mark Zuckerberg, é a responsável pelo gerenciamento e segurança do aplicativo, bem como a principal encarregada pela segurança das informações de seus usuários. Atualmente, utilizam um sistema de criptografia de ponta a ponta completa por padrão, permitindo apenas para o destinatário a leitura da mensagem enviada. De acordo com o BLOG DO WHATSAPP (2016), "Ninguém verá o conteúdo dessa mensagem. Nenhum cibercriminoso. Nenhum hacker. Nenhum regime opressivo. Nem mesmo nós".

No ano de 2024, o WhatsApp está sendo julgado pelo STF por uma liminar que derrubou bloqueio do aplicativo em 2016. Eles argumentaram na época, que deixaram de repassar as mensagens trocadas na plataforma porque representava uma quebra do sigilo. Isso representaria uma quebra da criptografia de "ponta a ponta", que impede terceiros de interceptar as conversas, e a apenas ao recebedor a sua leitura.

Em relação as eleições, o aplicativo afirma que estão comprometidos a combater abusos, e proteger a privacidade de seus usuários. No entanto, em casos de mensagens em massas,

serão aplicados banimentos.

De acordo com a META PLATFORMS INC.:

> O WhatsApp tem uma tecnologia de ponta para detectar spam que funciona 24h por dia. Nossa tecnologia identifica contas com comportamentos anormais para impedir que elas sejam utilizadas para espalhar spam ou desinformação. Por mês, nós banimos mais de 8 milhões de contas, e 75% delas são detectadas por nosso sistema automatizado. Nosso sistema impede o uso abusivo do WhatsApp antes mesmo que nossos usuários denunciem essas contas.

Para prevenção contra o uso abusivo de grupos, eles acrescentam, "desenvolvemos uma configuração de privacidade para que as pessoas possam decidir quem pode adicioná-las a grupos. As opções disponíveis são: *Todos*, *Meus contatos* ou *Meus contatos, exceto.*". Dessa forma, as pessoas podem limitar quem pode ou não adicioná-la a grupos.

No mundo digital, a criptografia se manifesta de diversas maneiras. Ela garante a confidencialidade das conversas no WhatsApp e em redes sociais, protege senhas de aplicativos e, também, impulsiona criptomoedas como Bitcoin e Ethereum, exigindo um poder computacional colossal para sua mineração. Assinaturas eletrônicas também se valem da criptografia para combater fraudes e falsificações, validando nossa identidade durante logins e transações bancárias.

Na troca de mensagens por e-mail, um dos programas utilizados é o PGP (Pretty Good Privacy), criado por Phil Zimmermann em 1991. De acordo com Gomes (2022, p. 21). "é um programa livremente disponível que usa a combinação do IDEA (criptografia de chave privada) com um protocolo RSA (chave pública), sendo o software de criptografia de e-mail mais utilizado no mundo".

Na época, a criptografia de chave pública já era utilizada por militares e grandes empresas. No entanto, o PGP teve um papel fundamental em tornar essa tecnologia acessível ao público em geral, ao contrário dos sistemas anteriores que eram caros e complexos. Phillip Zimmermann, o criador do PGP, enfrentou problemas com a justiça dos Estados Unidos por ter divulgado o código-fonte do programa na internet, o que violava leis de controle de exportação de armas. Segundo Costa e Figueiredo (2010, p. 19), "o governo americano incluía software de criptografia na categoria de armas e munições, junto com mísseis e metralhadoras". Por este motivo, Phillip não poderia ter tomado essa atitude sem a aprovação do departamento de defesa.

Ainda que a criptografia seja fundamental hoje em dia, sua relevância transcende eras. Desde os primórdios da comunicação humana, ela tem sido essencial para proteger mensagens, ordens reais e para contribuir para a segurança e o progresso da humanidade.

Atualmente, existem dois tipos de criptografia sendo utilizados: *simétrica* e *assimétrica*. Elas utilizam chaves para criptografar e descriptografar informações enviadas e recebidas. Além disso, é possível combiná-las, criando-se um *sistema criptográfico híbrido*.

A *criptografia simétrica* utiliza uma única chave para criptografar e descriptografar informações. Essa chave precisa ser compartilhada entre o remetente e o destinatário, o

que pode ser um desafio em termos de segurança e logística. No entanto, a simplicidade desse método o torna extremamente rápido e eficiente, ideal para criptografar grandes volumes de dados rapidamente.

Já a *criptografia assimétrica*, também conhecida como criptografia de chave pública, utiliza um par de chaves interligadas: pública e privada. A chave pública pode ser compartilhada livremente, enquanto a chave privada deve ser mantida em sigilo absoluto pelo destinatário. Essa assimetria permite diversas aplicações importantes, como: assinaturas digitais e troca segura de chaves. Aliás, um dos algoritmos de criptografia de chave pública mais comuns é o RSA, em que a sigla representa a inicial de seus criadores: Rivest, Shamir e Adleman.

Segundo Carneiro (2017, p. 20), "Adleman foi em grande parte responsável por detectar as falhas nas ideais de Rivest e Shamir, garantindo a estes que não perdessem tempo em pistas falsas". Já Rivest passava bastante tempo pensando na possibilidade de encontrar uma função de mão única que resolvesse a cifra assimétrica, conseguindo formalizar uma ideia de solução em 1977. Assim, com a parceria e trabalho colaborativo entre os três, em 1978, realizaram a criação do sistema RSA.

Em relação ao *sistema criptográfico híbrido*, ele combina os pontos fortes da criptografia simétrica e assimétrica. A chave assimétrica é usada para trocar com segurança uma chave simétrica temporária, que por sua vez é usada para criptografar grandes volumes de dados de forma eficiente. Essa combinação oferece a segurança robusta da criptografia assimétrica com o desempenho veloz da criptografia simétrica.

Apesar da criptografia assimétrica ser frequentemente associada à máxima segurança devido ao uso de chaves privadas, a verdadeira robustez de um sistema depende de um conjunto de fatores que vão além da assimetria. Segundo a IBM: "o comprimento e a complexidade das chaves"são os aspectos cruciais para a segurança da informação.

Para garantir a segurança e a privacidade dos dados de seus clientes, os bancos adotam sistemas de criptografia robustos. O Nubank, um dos bancos digitais em ascensão no Brasil, se destaca por investir em diversas camadas de proteção. De acordo com a NUBANK, "essas medidas englobam: criptografia de ponta a ponta, limitação de acessos, autenticação de dois fatores, reconhecimento biométrico e inteligência artificial (IA)."

Vale ressaltar que todo o processo de coleta, armazenamento e compartilhamento de dados dos clientes pelo Nubank é regido pela Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo a máxima transparência e segurança. Além disso, o banco mantêm o cliente atualizado sobre tudo o que acontece na conta por meio de e-mail ou notificações no aplicativo.

Uma ferramenta bastante utilizada nos últimos anos é o PIX, que é uma forma de fazer pagamentos ou transferências em apenas alguns segundos, em qualquer hora do dia de maneira instantânea, prática e segura. Com ele é possível pagar contas, agendar transações e sacar dinheiro. Segundo o BC (Banco Central do Brasil), o termo PIX foi escolhido por remeter a pixels, tecnologias e transações.

Para utilizar o PIX é necessário uma chave que pode ser o CPF/CNPJ, e-mail, número de celular ou até mesmo criar uma chave aleatória. O BC afirma que as "pessoas físicas podem cadastrar até 5 chaves para cada conta. E pessoas jurídicas, até 20 chaves."Além disso, para realizar pagamentos ou recebimentos via PIX, uma das opções é o uso de QR-Code (Quick Response Code - Código de resposta rápida). O seu funcionamento é parecido com o do código de barras, mas com um "upgrade"que possibilita uma infinidade de ações digitais.

A Figura 1.10 apresenta um exemplo de QR - Code, o código é referente ao canal de Matemática do YouTube: Me ajuda Du.

Figura 1.10: QR-Code

Fonte: QR-CODE FÁCIL.

Para as próximas gerações, a criptografia de curva elíptica (ECC) se destaca como uma das tecnologias mais promissoras para garantir a segurança da informação. Essa técnica de criptografia de chave pública, baseada na matemática das curvas elípticas, oferece diversas vantagens em relação aos sistemas tradicionais: maior rapidez, menor tamanho e eficiência aprimorada.

De acordo com a IBM:

> Os sistemas criptográficos de chave pública de primeira geração são baseados em funções matemáticas de multiplicação e fatoração, nas quais as chaves pública e privada revelam as funções matemáticas específicas necessárias tanto para cifrar o texto simples quanto para decifrar o texto cifrado. Essas chaves são feitas multiplicando os números primos. O ECC utiliza curvas elípticas - equações que podem ser representadas como linhas curvas em um grafo - para gerar chaves públicas e privadas com base em diferentes pontos no gráfico de linha.

Com o crescente volume de dados digitais e a sofisticação das ameaças cibernéticas, a ECC se torna essencial para proteger informações confidenciais e garantir a privacidade em um mundo cada vez mais digital. Em breve, a ECC poderá se tornar o novo padrão de segurança, apesar da crescente ameaça dos computadores quânticos (que estão em estado inicial e são difíceis de construir, programar e de custear) que podem tornar obsoletos os sistemas tradicionais.

O computador quântico traz uma preocupação enorme aos criptógrafos devido a sua potencial ameaça aos protocolos criptográficos atuais, que poderão torna-se ultrapassados. Por essa razão, surge a busca por algoritmos que não possam ser quebrados por computadores quânticos, aparece, assim, o movimento pós-quântico. Para Araujo (2018, p. 92), "uma das propostas mais importantes fundamenta-se em problemas envolvendo reticulados algébricos, tais como o problema do vetor mais curto e o problema do vetor mais próximo".

A criptografia, com sua história milenar que remonta aos primórdios da humanidade, vem sendo aprimorada incansavelmente ao longo dos anos, impulsionada pela busca incessante por um nível cada vez mais elevado de segurança da informação. No entanto, sempre haverão cibercriminosos em busca dessas informações. Como afirma Singh (2001, p. 345), "esta sempre foi uma corrida apertada, com os decifradores contra-atacando sempre que os criadores de códigos pareciam está ganhando, e estes anteriores não eram mais confiáveis.".

Embora o computador quântico ainda esteja em sua fase inicial, diversos métodos de criptografia já se encontram em uso, como o RSA e a ECC, esta última se apresentando como uma alternativa promissora para o futuro próximo. Apesar de ser mais recente, muitos ainda optam pelo sistema RSA. De acordo com Arruda (2014, p. 28), "o algoritmo ECC oferece segurança equivalente ao RSA com o uso de chaves menores, o que resulta na redução da carga de processamento durante os cálculos criptográficos".

Para uma melhor compreensão do processo de criptografia, os próximos capítulos abordarão temas essenciais que contribuirão para a desmistificação de um cripto-sistema. Nessa jornada, serão vistos temas que ajudarão nas etapas de compreensão dos processos de criptografia e descriptografia do Sistema RSA, por exemplo, lançando luz sobre os mecanismos que garantem a segurança das informações. Também será visto um pouco sobre o algoritmo de curvas elípticas (ECC).

Capítulo 2

Conceitos básicos para Compreensão de um Cripto-sistema

A Aritmética, como um pilar fundamental, sustenta a construção do conhecimento em Criptografia. Sua jornada inicia-se com o estudo das propriedades dos números inteiros, para o entendimento de suas definições e, assim, conseguir abrir caminho para temas mais complexos. Entre eles, destaca-se a Relação de Ordem, que ordena os números de forma lógica, e o Princípio da Boa Ordenação (PBO), que garante a existência de um menor elemento em cada conjunto não vazio. A Divisibilidade (Divisão Euclidiana) completa o quadro, permitindo a análise da divisibilidade entre números, um conceito crucial no funcionamento do sistema RSA (método criptográfico mais utilizado na atualidade), que utiliza um par de chaves, pública e privada, para garantir a segurança da comunicação.

A história dos números é tão rica que se entrelaça com o desenvolvimento da sociedade. O conceito de número, por exemplo, surgiu da necessidade vital de quantificar animais, objetos e elementos do cotidiano nas civilizações antigas, dando origem aos números naturais. Com o tempo, a crescente demanda por controle e registro de mercadorias conduziu para a criação dos números negativos, expandindo o universo numérico. Essa evolução constante dos conjuntos numéricos acompanha a trajetória da humanidade, impulsionada pela busca incessante por aperfeiçoamento de técnicas, cálculos e soluções eficientes para os desafios que surgem.

Desse modo, utilizando o livro de Aritmética (HEFEZ, 2022) como guia, será feito um estudo das propriedades dos números inteiros, como adição e multiplicação. Posteriormente, uma investigação dos Princípios da Boa Ordenação e da Indução Matemática, ferramentas poderosas para provar teoremas e fazer generalizações. E, para finalizar, uma análise criteriosa da divisibilidade, especificamente a Divisão Euclidiana.

2.1 Números Inteiros ($\mathbb{Z}$)

O Conjunto dos Números Inteiros é representado pelo símbolo $\mathbb{Z}$, referente à palavra alemã *Zahlen*, que significa números ou algarismos. Pode-se denotar o Conjunto dos Números Inteiros como:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Observe que o Conjunto é formado por valores negativos (-), positivos (+) e pelo zero (que não possui sinal). Entre os subconjuntos próprios dos Inteiros, o que mais se destaca são os Naturais (Conjunto dos Números Naturais), representado por $\mathbb{N}$ e obtido por: $\mathbb{Z}_+ = \{0, 1, 2, 3, \dots\}$.

Embora os Naturais sejam considerados com o zero como ponto de partida do conjunto, para demonstrações e uso dos Axiomas de Peano, consideremos o Conjunto dos Números Naturais inciando a partir do 1, pois para Peano o zero não é considerado um número natural. Assim, têm-se:

$$\mathbb{N} = \mathbb{Z}_+ = \{1, 2, 3, 4, 5, 6, 7, 8, 9, \dots\}.$$

2.1.1 Propriedades

As operações de adição e multiplicação dos Números Inteiros ($\mathbb{Z}$) possuem as seguintes propriedades:

(i) A adição e a multiplicação são bem definidas: $\forall a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

(ii) Comutativa: $\forall a, b \in \mathbb{Z}$; $a + b = b + a$ e $a \cdot b = b \cdot a$.

(iii) Associativa: $\forall a, b \in \mathbb{Z}$; $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iv) Elementos neutros: $\forall a \in \mathbb{Z}$; $a + 0 = 0 + a = a$ e $a \cdot 1 = 1 \cdot a = a$.

(v) A adição possui elemento simétrico: $\forall a \in \mathbb{Z}$, $\exists\ (-a) \in \mathbb{Z}$ tal que $a + (-a) = 0$.

(vi) A multiplicação é distributiva com relação à adição: $\forall a, b, c \in \mathbb{Z}$; $a \cdot (b + c) = a \cdot b + a \cdot c$.

Ao aplicar as Propriedades 2.1.1, juntamente com suas operações de adição e multiplicação, outros Conjuntos Numéricos se submetem às leis básicas da aritmética. De acordo com Hefez (2022, p. 3), essa estrutura, na terminologia moderna, é denominada "anel". Portanto, as propriedades descritas caracterizam o conjunto $(\mathbb{Z}, +, \cdot)$ como um anel.

Vale salientar que os Números Racionais ($\mathbb{Q}$) e Reais ($\mathbb{R}$), com suas respectivas operações de adição e multiplicação, também se configuram como anéis. No entanto, este trabalho dará ênfase aos Números Inteiros, com menções pontuais aos Números Racionais e Reais.

2.1.2 Adição e Multiplicação

As Propriedades 2.1.1 tem como consequência as Proposições a seguir:

Proposição 1. $\forall a \in \mathbb{Z}$, $a \cdot 0 = 0$.

Demonstração. Seja $b \in \mathbb{Z}$. Pela Propriedade do elemento simétrico (v), têm-se que $b + (-b) = 0$. Assim, substituindo na Proposição, segue-se:

$$\begin{aligned} a \cdot 0 &\overset{(v)}{=} a \cdot (b + (-b)) && \text{(Elemento simétrico)} \\ &\overset{(vi)}{=} ab + (-ab) && \text{(Propriedade distributiva)} \\ &= k + (-k) && \text{(Tomando } k = a \cdot b, \text{ com } k \in \mathbb{Z}) \\ &\overset{(v)}{=} 0 && \text{(Elemento simétrico)} \end{aligned}$$

$\therefore \forall a \in \mathbb{Z}, \quad a \cdot 0 = 0.$

■

Proposição 2. O elemento neutro da adição é único.

Demonstração. Suponha que 0 e 0' sejam elementos neutros da adição, com 0, $0' \in \mathbb{Z}$. Assim, dá-se:

$$1.\ \forall a \in \mathbb{Z} \mid a + 0 = a.$$

$$2.\ \forall a \in \mathbb{Z} \mid a + 0' = a.$$

Aplicando a propriedade do elemento neutro da adição (iv) nas equações (1) e (2), têm-se:

$$3.\ 0' + 0 = 0'$$
$$4.\ 0 + 0' = 0$$

Agora, relacionando (3) e (4) a partir da propriedade comutativa, obtêm-se:

$$0' + 0 = 0 + 0' \Rightarrow 0' = 0.$$

Portanto, o elemento neutro da adição é único.

■

Proposição 3. A adição é compatível e cancelativa com respeito à igualdade. $\forall a, b, c \in \mathbb{Z}$, $a = b \Leftrightarrow a + c = b + c$.

Demonstração.

($\Rightarrow$) Como $a = b$, basta adicionar c em ambos os lados da igualdade:

$$a = b \Rightarrow a + c = b + c, \text{ com } c \in \mathbb{Z}.$$

($\Leftarrow$) Sabe-se que $a + c = b + c$. Pela propriedade do elemento simétrico (v), como $c \in \mathbb{Z}$, $\exists\ (-c) \in \mathbb{Z}$ tal que $c + (-c) = 0$. Assim, adicionando $(-c)$ em ambos os lados, chega-se em: $a + c = b + c \Rightarrow a + c + (-c) = b + c + (-c) \overset{(v)}{\Rightarrow} a + 0 = b + 0 \overset{(iv)}{\Rightarrow} a = b$.

$\therefore \forall a, b, c \in \mathbb{Z}$, $a = b \Leftrightarrow a + c = b + c$.

■

Vale ressaltar que de acordo com o formado da ordenação nos Inteiros ($\mathbb{Z}$), valem às seguintes propriedades:

(vii) Fechamento de $\mathbb{N}$: O Conjunto dos Números Naturais é fechado tanto para adição quanto para multiplicação. Isto ocorre porque quando realiza-se a adição entre dois números naturais o resultado sempre é um número natural e quando realiza-se o produto entre naturais o resultado também é sempre um natural. Assim, $\forall a, b \in \mathbb{N}$, têm-se que $a + b \in \mathbb{N}$ e $a \cdot b \in \mathbb{N}$.

(viii) Tricotomia: é um método de comparação entre dois números, em que a relação entre eles possui três situações possíveis. Havendo, entre elas, apenas uma possibilidade verificada:

(a) $a = b$;

(b) $b - a \in \mathbb{N}$;

(c) $-(b - a) = a - b \in \mathbb{N}$.

Definição 1. $a < b$, toda vez que $b - a \in \mathbb{N}$.

Definição 2. $a > b$, toda vez que $a - b \in \mathbb{N}$.

Com estas definições, pode-se afirmar que na tricotomia dados $a, b \in \mathbb{Z}$, uma, e somente uma, das seguintes condições é verificada:

(a) $a = b$;

(b) $a < b \overset{\text{Def.1}}{\Leftrightarrow} b - a \in \mathbb{N}$;

(c) $b < a \overset{\text{Def.2}}{\Leftrightarrow} a - b \in \mathbb{N}$.

Note que como $a - 0 = a$, têm-se, a partir das definições, que $a > 0$ se, e somente se, $a \in \mathbb{N}$. Desta forma, $\{x \in \mathbb{Z}; x > 0\} = \mathbb{N}$ e $\{x \in \mathbb{Z}; x < 0\} = -\mathbb{N}$.

Definição 3. Diz-se que um anel A é um *Domínio de Integridade* se a propriedade seguinte for válida: $\forall a, b \in \mathbb{Z}$, tais que $a \cdot b = 0$, então $a = 0$ ou $b = 0$.

Exemplo 1. $\forall a, b, c \in \mathbb{Z}$ $(c \neq 0)$, Se $a = b \Leftrightarrow a \cdot c = b \cdot c$.

Demonstração. ($\Rightarrow$) Por hipótese, $a = b$. Assim, se $c \in \mathbb{Z}(c \neq 0)$, pela propriedade do fechamento multiplicativo (vii), segue-se: $a = b \overset{\cdot c}{\Rightarrow} a \cdot c = b \cdot c$. Note que aqui $c = 0$ é válido.

($\Leftarrow$) Será utilizado a tricotomia para provar a volta. Assim, por hipótese, $a \cdot c = b \cdot c$. Como $c \neq 0$, existem duas possibilidades para serem analisadas:

$$\begin{cases} c > 0; \\ -c > 0, \text{ pois se } c < 0 \Rightarrow -c > 0. \end{cases}$$

(i) $c > 0$:

(a) Se $a < b \overset{\text{Def.1}}{\Rightarrow} b - a \in \mathbb{N}$. Assim, se $c \in \mathbb{N}$, pelo fato dos $\mathbb{N}$ serem fechados multiplicativamente (vii), obtêm-se:
$(b-a) \cdot c \in \mathbb{N} \overset{\text{(vi)}}{\Rightarrow} bc - ac \in \mathbb{N} \overset{\text{Def.1}}{\Rightarrow} a \cdot c < b \cdot c$, que é um absurdo.

(b) Se $a > b \overset{\text{Def.2}}{\Rightarrow} a - b \in \mathbb{N}$. Desse modo, se $c \in \mathbb{N}$, pelo fato dos $\mathbb{N}$ serem fechados para multiplicação (vii), têm-se:
$(a-b) \cdot c \in \mathbb{N} \overset{\text{(vi)}}{\Rightarrow} ac - bc \in \mathbb{N} \overset{\text{Def.2}}{\Rightarrow} b \cdot c < a \cdot c$, que também é um absurdo.

(c) Logo $a = b$.

(ii) $-c > 0$:

(a) Se $a < b \overset{\text{Def.1}}{\Rightarrow} b - a \in \mathbb{N}$. Assim, se $-c \in \mathbb{N}$, pelo fato dos $\mathbb{N}$ serem fechados para multiplicação (vii), obtêm-se:
$(b-a) \cdot (-c) \in \mathbb{N} \overset{\text{(vi)}}{\Rightarrow} -bc + ac \in \mathbb{N} \overset{\text{(ii)}}{\Rightarrow} ac - bc \in \mathbb{N} \overset{\text{Def.2}}{\Rightarrow} b \cdot c < a \cdot c$, que é um absurdo.

(b) Se $a > b \overset{\text{Def.2}}{\Rightarrow} a - b \in \mathbb{N}$. Desse modo, se $-c \in \mathbb{N}$, pelo fato dos $\mathbb{N}$ serem fechados para multiplicação (vii), têm-se:
$(a-b) \cdot (-c) \in \mathbb{N} \overset{\text{(vi)}}{\Rightarrow} -ac + bc \in \mathbb{N} \overset{\text{(ii)}}{\Rightarrow} bc - ac \in \mathbb{N} \overset{\text{Def.1}}{\Rightarrow} a \cdot c < b \cdot c$, que também é um absurdo.

(c) Logo, a única possibilidade válida é $a = b$.

$\therefore \forall a, b, c \in \mathbb{Z}$ (com $c \neq 0$), $a = b \Leftrightarrow ac = bc$.

■

2.1.3 Relação de ordem

Os Números Inteiros ($\mathbb{Z}$) podem ser comparados entre si através de uma relação de ordem. Essa ordenação permite determinar qual número é maior, menor ou igual a outro. Para conseguir entender essa relação, pode-se imaginar essa ordenação em uma reta numérica, onde cada ponto representa um número inteiro. Assim, a posição de cada número na reta determinará sua característica: quanto mais à direita um número estiver na reta, maior ele será, e quanto mais à esquerda, menor ele será.

Além disso, para que uma relação seja de fato considerada uma *Relação de Ordem*, ela precisa atender a três propriedades fundamentais: reflexiva, antissimétrica e transitiva.

Definição 4. Seja A um conjunto não nulo, com $a, b, c \in A$, e seja R uma relação definida em A. Para que R seja uma *Relação de Ordem*, precisa-se satisfazer as seguintes propriedades:

(i) Reflexiva: $\forall a \in A$; aRa.

(ii) Antissimétrica: $\forall a, b \in A$. Se aRb e $bRa \Rightarrow a = b$.

(iii) Transitiva: $\forall a, b, c \in A$. Se aRb e $bRc \Rightarrow aRc$.

Outra forma de representar essa relação de ordem é a seguinte:

(i) Reflexiva: $\forall a \in \mathbb{Z}$, $a \leq a$.

(ii) Antissimétrica: $\forall a, b \in \mathbb{Z}$, $a \leq b$ e $b \leq a \Rightarrow a = b$.

(iii) Transitiva: $\forall a, b, c \in \mathbb{Z}$, $a \leq b$ e $b \leq c \Rightarrow a \leq c$.

Proposição 4. A relação "menor do que"é transitiva (Transitividade): $\forall a, b, c \in \mathbb{Z}$, $a < b$ e $b < c \Rightarrow a < c$.

Demonstração. Por hipóteses, $\begin{cases} a < b \overset{\text{Def.1}}{\Rightarrow} \ b - a \in \mathbb{N} \\ b < c \overset{\text{Def.1}}{\Rightarrow} \ c - b \in \mathbb{N} \end{cases} \overset{\text{(vii)}}{\Rightarrow} \ (b-a) + (c-b) \in \mathbb{N} \overset{\text{(ii) e (iii)}}{\Rightarrow}$

$(b + (-b)) + (c - a) \in \mathbb{N} \overset{\text{(v)}}{\Rightarrow} \ 0 + (c - a) \in \mathbb{N} \overset{\text{(iv)}}{\Rightarrow} \ c - a \in \mathbb{N} \overset{\text{Def.1}}{\Rightarrow} \ a < c.$

$\therefore \forall a, b, c \in \mathbb{Z}$, se $a < b$ e $b < c \Rightarrow a < c$.

■

Proposição 5. A adição é compatível e cancelativa com respeito à relação "menor do que": $\forall a, b, c \in \mathbb{Z}$, $a < b \Leftrightarrow a + c < b + c$.

Demonstração. ($\Rightarrow$) Por hipótese, $a < b \overset{\text{Def.1}}{\Rightarrow} \ b - a \in \mathbb{N}$. Utilizando-se do fato de $c + (-c) \overset{\text{(v)}}{=} 0$, devido a propriedade do elemento simétrico, têm-se:

$$b - a + c + (-c) \in \mathbb{N} \overset{\text{(ii) e (iii)}}{\Rightarrow} \ (b + c) - (a + c) \in \mathbb{N} \overset{\text{Def.1}}{\Rightarrow} \ a + c < b + c.$$

($\Leftarrow$) Reciprocamente, suponha $a + c < b + c$. Adicionando $(-c) \in \mathbb{Z}$ em ambos os lados da desigualdade, obtêm-se: $a + c + (-c) < b + c + (-c) \overset{\text{(v)}}{\Rightarrow} \ a + 0 < b + 0 \overset{\text{(iv)}}{\Rightarrow} \ a < b$.

■

Proposição 6. A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação "menor do que": $\forall a, b \in \mathbb{Z}, \forall c \in \mathbb{N}$, $a < b \Leftrightarrow a \cdot c < b \cdot c$.

Demonstração. ($\Rightarrow$) Por hipótese, $a < b \overset{\text{Def.1}}{\Rightarrow} \ b - a \in \mathbb{N}$. Como $c \in \mathbb{N}$, pela propriedade do fechamento multiplicativo (viii), têm-se: $(b-a) \cdot c \in \mathbb{N} \overset{\text{(vi)}}{\Rightarrow} \ bc - ac \in \mathbb{N} \overset{\text{Def.1}}{\Rightarrow} \ a \cdot c < b \cdot c$. Logo, $ac < bc$.

($\Leftarrow$) De forma recíproca, por hipótese $a \cdot c < b \cdot c$, com $c \in \mathbb{N}$. Utilizando tricotomia, têm-se três possibilidades para verificar:

1. Suponha que se $a \cdot c < b \cdot c$ então $a = b$. No entanto, se $a = b \overset{\cdot c}{\Rightarrow} \ a \cdot c = b \cdot c$. Falso por hipótese.

2. Suponha que se $a \cdot c < b \cdot c$ então $b < a$. Mas, se $b < a \overset{\cdot c}{\Rightarrow} \ b \cdot c < a \cdot c$. Falso por hipótese.

3. Logo, só resta a possibilidade de $a < b$.

■

Definição 5. Valor absoluto: Seja $a \in \mathbb{Z}$, define-se: $\mid a \mid = \begin{cases} a, \text{ se } a \geq 0 \\ -a, \text{ se } a < 0. \end{cases}$

Note que $\forall a \in \mathbb{Z}$, têm-se que $\mid a \mid \geq 0$ e $\mid a \mid = 0$ se, e somente se, $a = 0$. Além disso, chama-se de *módulo* ou *valor absoluto* de a o número inteiro $\mid a \mid$.

Pode-se ver a seguir algumas propriedades básicas do módulo:

Proposição 7. $\forall a, b \in \mathbb{Z}$ e $r \in \mathbb{N}$, têm-se:

(i) $\mid a \cdot b \mid = \mid a \mid \cdot \mid b \mid$;

(ii) $\mid a \mid \leq r$ se, e somente se, $-r \leq a \leq r$;

(iii) $- \mid a \mid \leq a \leq \mid a \mid$;

(iv) a desigualdade triangular: $\mid \mid a \mid - \mid b \mid \mid \leq \mid a \pm b \mid \leq \mid a \mid + \mid b \mid$.

As demonstrações das propriedades do módulo serão mostradas a seguir:

Demonstração (i): Como $\mid a \cdot b \mid^2 = (a \cdot b)^2 = a^2 \cdot b^2 = \mid a \mid^2 \cdot \mid b \mid^2 \Rightarrow \mid ab \mid = \pm \mid a \mid \cdot \mid b \mid$. Pela definição de módulo, $\mid a \mid \geq 0$. Logo, $\mid a \cdot b \mid = \mid a \mid \cdot \mid b \mid$.

■

Demonstração (ii): Pela definição de módulo (Definição 5), sabe-se que:

$$\forall a \in \mathbb{Z} \text{ e } r \in \mathbb{N}; \mid a \mid < r \Leftrightarrow a < r \text{ e } a > -r.$$

$(\Rightarrow)$ Pela Definição 5, $\begin{cases} \mid a \mid < r \\ - \mid a \mid > -r \end{cases} \Rightarrow -r < - \mid a \mid < a < \mid a \mid < r \Rightarrow -r < a < r.$

$(\Leftarrow)$ Precisa-se analisar dois casos: $a < r$ e $a > -r$.

1° caso $(a > 0)$: $\mid a \mid = a < r \Rightarrow \mid a \mid < r$.

2° caso $(a < 0)$: $\mid a \mid = -a < r \Rightarrow \mid a \mid = a > -r \Rightarrow \mid a \mid > -r$.

$\therefore \forall r \in \mathbb{N}$ e $a \in \mathbb{Z}$; $\mid a \mid < r \Leftrightarrow -r < a < r$.

■

Demonstração (iii): Precisa-se verificar dois casos possíveis:

1° caso: Para $a \geq 0$, pela definição de módulo, têm-se que: $\mid a \mid = a \Rightarrow - \mid a \mid < 0$. Logo, como a não é negativo, $- \mid a \mid \leq a \leq \mid a \mid$.

2° caso: Com $a < 0$, pela definição de módulo, segue-se que: $\mid a \mid = -a \Rightarrow - \mid a \mid = a \Rightarrow - \mid a \mid < 0 \Rightarrow \mid a \mid > 0$. Assim, $- \mid a \mid = -(-a) \leq a \leq \mid a \mid$. Logo, como a é negativo, $- \mid a \mid \leq a \leq \mid a \mid$.

■

Demonstração (iv): Elevando $| a + b |$ ao quadrado, obtêm-se:

$$| a + b |^2 = (a + b)^2 = a^2 + 2ab + b^2 \leq | a |^2 + 2 | a | \cdot | b | + | b |^2 = (| a | + | b |)^2$$
$$\overset{(vi)}{\Rightarrow} | a + b |^2 \leq (| a | + | b |)^2 \Rightarrow | a + b | \leq (| a | + | b |)$$

$$\therefore | a + b | \leq (| a | + | b |)$$

Para $| a - b | \leq (| a | + | b |)$ a demonstração é análoga.

■

2.2 Princípio da Boa Ordenação - PBO

O Princípio da Boa Ordenação (PBO) estabelece que todo subconjunto não vazio de números naturais possui um menor elemento. Essa propriedade fundamental da ordenação dos números naturais será explorada neste estudo, com base no livro *Curso de Análise (Volume 1)* do Professor Elon Lages Lima (LIMA, 2022).

Seja A um subconjunto não vazio de números naturais ($A \subset \mathbb{N}$). Diz-se que um número $n_0 \in A$ é o *menor elemento* de A (ou *elemento mínimo de A*) quando se tem $n_0 \leq a$ para todo $a \in A$. Por exemplo, o 1 é o menor elemento do conjunto $\mathbb{N}$ de todos os naturais existentes (pois o zero não faz parte dos $\mathbb{N}$ de acordo com Giuseppe Peano). Assim, independente do subconjunto não vazio, qualquer que seja $A \subset \mathbb{N}$ com $1 \in A$, 1 é o menor elemento de A.

Proposição 8. *Seja $A \subset \mathbb{N}$ um subconjunto não vazio então A tem um único menor elemento. Logo, o menor elemento de um conjunto é único.*

De forma análoga, diz-se que $m \in A$ é o *maior elemento* de A (ou *elemento máximo* de A) quando se tem $m \geq n$ para todo $n \in A$. No entanto, nem todo conjunto formado por números naturais possui um maior elemento, o próprio Conjunto dos Números Naturais não possui maior elemento, pois para todo $n \in \mathbb{N}$ sempre encontra-se um sucessor de n, que é o $n + 1$.

Teorema 1. (*Princípio da Boa Ordenação*). Todo subconjunto não vazio $A \subset \mathbb{N}$ possui um *elemento mínimo*, isto é, existe um elemento $n_0 \in A$ tal que $n_0 \leq n$ para todo $n \in A$.

Demonstração. Considere o conjunto $I_n = \{m \in \mathbb{N}; m \leq n\}$, ou seja, I_n é um conjunto formado por números naturais que são menores ou iguais a n. Por exemplo, $I_3 = \{1, 2, 3\}$.

Precisa-se analisar dois casos possíveis:

(i) Suponha que $1 \in A$. Pelo segundo axioma de Peano, 1 é o único número natural que não é sucessor de ninguém.

Para que $\exists\ n_0 \in \mathbb{N}$ tal que $n_0 < 1 \Rightarrow \exists m \in \mathbb{N}$ tal que $1 = n_0 + m = s(n_0)$, em que $s(n_0)$ é o sucessor de n_0 e m o que falta para n_0 chegar em 1. Absurdo, pois o 1 não é sucessor de ninguém.

Portanto, o 1 é o menor elemento de A.

(ii) Suponha que $1 \notin A$: Considere o conjunto $X = \{n \in \mathbb{N}; I_n \subset \mathbb{N} - A\}$, ou seja, é formado pelos números $n \in \mathbb{N}$ tais que $I_n \subset \mathbb{N} - A$, e I_n encontra-se no complementar de A.

Note que $X \neq \emptyset$ e que $1 \in X$. Assim, $1 \notin A$ e, portanto, $1 \in \mathbb{N} - A$.

Como $I_1 = \{1\} \Rightarrow I_1 \subset \mathbb{N} - A$, pois $1 \in X$. Em contrapartida, como $A \neq \emptyset$, segue-se que $X \neq \mathbb{N}$. Logo, o terceiro axioma de Peano não é válido.

- Terceiro Axioma de Peano: Se $X \in \mathbb{N}$ é tal que $1 \in X$ e $S(n) \in X$, $\forall n \in X$ $\Rightarrow X = \mathbb{N}$.

Como $1 \in X$, mas $X \neq \mathbb{N} \Rightarrow \exists\ n \in X$ tal que $S(n) \notin X$. Desta maneira, $I_n = \{1, 2, 3, \ldots, n\} \subset \mathbb{N}$, mas $S(n) = n + 1 = n_0$, com $n_0 \in A$. Logo, n_0 é o menor elemento de A.

Para mostrar que n_0 é o menor elemento de A: Suponha por absurdo que $\exists\ a \in A$ tal que $a < n_0 \Rightarrow n_0 = a + m$ para algum $m \in \mathbb{N}$.

Como $n_0 = n+1 \Rightarrow n+1 = n_0 = a+m$. Desta forma, precisa-se verificar dois casos:

1° caso: Se $m = 1 \Rightarrow n + 1 = a + 1 \overset{(-1)}{\Rightarrow}\ n + 1 + (-1) = a + 1 + (-1) \overset{(v)}{\Rightarrow}\ n = a$

$\Rightarrow a \in I_n \Rightarrow a \in X \subset \mathbb{N} - A$. Absurdo, pois por hipótese $a \in A$.

2° caso: Se $m \neq 1 \Rightarrow$ que m é sucessor de algum número $p \in \mathbb{N}$, isto é, $m = p + 1$.

Dessa maneira, $n + 1 = n_0 = a + m \Rightarrow n + 1 = a + (p + 1) \overset{(v)}{\Rightarrow}\ n = a + p \Rightarrow a < n$

$\Rightarrow a \in I_n \Rightarrow a \in X \subset \mathbb{N} - A$. Absurdo novamente.

Portanto, n_0 é o menor elemento de A.

■

Outro princípio importante para os números naturais é o da *Indução matemática*. Enquanto o *Princípio da Boa Ordenação (PBO)* garante que todo subconjunto não vazio dos naturais possui um menor elemento, o *Princípio da Indução Matemática* fornece um método para mostrar que uma propriedade é válida para todos os números naturais.

2.3 Princípios de Indução Matemática

O instrumento a seguir é uma importante ferramenta que elenca os passos para realização de demonstrações de teoremas:

Teorema 2. (Princípio de Indução Matemática Fraca) Seja $a \in \mathbb{Z}$ e seja $p(n)$ uma sentença aberta em n. Suponha que

(i) $p(a)$ é verdadeiro, e que

(ii) $\forall n \geq a$, $p(n) \Rightarrow p(n+1)$ é verdadeiro.

Então, $p(n)$ é verdadeiro para todo $n \geq a$.

O Princípio de Indução Matemática admite uma variante, chamada de Princípio da Indução Matemática Completa, ou Princípio da Indução Matemática Forte, ou Segunda Forma do Princípio de Indução Matemática, que é bastante útil quando a Indução Fraca não é suficiente para demonstração:

Teorema 3. (Princípio de Indução Matemática Forte) Seja $p(n)$ uma sentença aberta em n tal que

(i) $p(a)$ é verdadeiro, e que

(ii) $\forall n$, $p(a)$ e $p(a+1)$ e $\cdots$ e $p(n) \Rightarrow p(n+1)$ é verdadeiro.

Então, $p(n)$ é verdadeiro para todo $n \geq a$.

As demonstrações dos Princípios de Indução podem ser encontradas no livro de Aritmética de Hefez (2022, p. 11 - 13).

Exemplo 2. Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Prove que $(a+b)$ divide $(a^{2n} - b^{2n})$, usando indução matemática. Observação: será usado a barra vertical ($|$) para representar a divisibilidade.

Demonstração. Vamos provar por indução matemática fraca:

(i) Verificar para $n = 1$: $(a+b) \mid (a^2 - b^2)$, pois $(a+b) \mid (a+b) \cdot (a-b)$. Assim, é verdadeira para $n = 1$.

(ii) (Hipótese de indução) Suponha que $(a+b) \mid (a^{2n} - b^{2n})$ para algum $n \in \mathbb{N}$.

(Tese) Deseja-se provar que $a+b \mid a^{2(n+1)} - b^{2(n+1)}$.

(iii) Note que

$$\begin{aligned} a^{2(n+1)} - b^{2(n+1)} &= a^{2n+2} - b^{2n+2} \\ &= a^{2n} \cdot a^2 - b^{2n} \cdot b^2 \\ &= a^{2n}a^2 - a^{2n}b^2 + a^{2n}b^2 - b^{2n}b^2 && \text{(Elemento simétrico)} \\ &= a^{2n}(a^2 - b^2) + b^2(a^{2n} - b^{2n}) && \text{(Distributiva)} \end{aligned}$$

Como $a+b \mid a^2 - b^2$ *em (i)* e $a+b \mid a^{2n} - b^{2n}$ (por hipótese) $\Rightarrow a+b \mid a^{2(n+1)} - b^{2(n+1)}$.

Logo, a propriedade é verdadeira para $n+1$.

Portanto, pelo Princípio de Indução Matemática Fraca, $a+b \mid a^{2n} - b^{2n}$ para todo $n \in \mathbb{N}$.

■

Uma aplicação importante do *princípio de indução* é na área da teoria dos números, especificamente em questões envolvendo a divisibilidade. Pode-se utilizar a indução, por exemplo, para mostrar que uma determinada expressão é divisível por um número ou por outra expressão dada (como o realizado no exemplo anterior). Além disso, esse método de prova possibilita generalizar propriedades de divisibilidade a partir de casos particulares.

2.4 Divisibilidade

A divisibilidade é um conceito fundamental estudado desde o Ensino Fundamental. Nessa fase, aprende-se a analisar os critérios de divisibilidade por diversos números. Um exemplo clássico é o critério de divisibilidade por 2, em que basta verificar se o número é par, ou seja, se termina em 0, 2, 4, 6 ou 8. Aplicando esse critério, pode-se facilmente concluir que o número 2024 é divisível por 2, pois termina em 4.

No entanto, a aritmética modular vai além da simples divisibilidade. Ela se concentra na análise dos restos da divisão de um número inteiro por outro. Esses restos, muitas vezes negligenciados, revelam informações valiosas e abrem um universo de possibilidades matemáticas intrigantes, como, por exemplo, a sua aplicação em Criptografia RSA.

Definição 6. Sejam a e b inteiros, com $a \neq 0$. Se existir um inteiro c tal que $b = ac$, diz-se que a divide b, ou que b é múltiplo de a.

Notação 1. $a \mid b$ indica que a divide b, e a negação, a não divide b, é indicada por $a \nmid b$.

Proposição 9. Sejam $a, b, c \in \mathbb{Z}$. Tem-se que

(i) $1 \mid a$, $a \mid a$ e $a \mid 0$.

(ii) $0 \mid a \Rightarrow a = 0$.

(iii) $a \mid b$ se, e somente se, $\mid a \mid$ divide $\mid b \mid$.

(iv) se $a \mid b$ e $b \mid c$, então $a \mid c$.

Pode-se encontrar as demonstrações (i) a (iv) no livro de Aritmética de Hefez (2022, p. 32 - 33). Aqui será visto que a relação de divisibilidade em $\mathbb{N} \cup \{0\}$ é uma relação de ordem, isto é, a divisibilidade é reflexiva, transitiva e assimétrica. Além disso, também serão mostradas proposições importantes para o entendimento de algumas demonstrações.

Proposição 10. (Reflexiva) $\forall a \in \mathbb{N} \cup \{0\}$, $a \mid a$.

Demonstração. Note que, tomando $c = 1$ ($c \in \mathbb{Z}$), obtém-se: $a = 1 \cdot a$, pois 1 é elemento neutro multiplicativo.

$\therefore \exists c \in \mathbb{Z} / a = ca \overset{\text{Def.6}}{\Leftrightarrow} a \mid a$.

■

Proposição 11. (Transitividade) $\forall a, b, c \in \mathbb{N} \cup \{0\}$, se $a \mid b$ e $b \mid c \Rightarrow a \mid c$.

Demonstração. Por hipóteses, $\begin{cases} a \mid b \overset{\text{Def.6}}{\Rightarrow} \exists\ p \in \mathbb{Z} \text{ tal que } b = a \cdot p\ (i) \\ b \mid c \overset{\text{Def.6}}{\Rightarrow} \exists\ q \in \mathbb{Z} \text{ tal que } c = b \cdot q\ (ii) \end{cases}$

Como $c = b \cdot q \overset{(i)}{\Rightarrow} c = (ap) \cdot q \overset{associativa}{=} a \cdot (pq) \overset{fechamento}{=} a \cdot k$, com $k = pq$.

Logo, $c = ak$ $(k \in \mathbb{Z})$.

$\therefore a \mid c$.

■

Proposição 12. (Antissimétrica) $\forall a, b \in \mathbb{N} \cup \{0\}$, se $a \mid b$ e $b \mid a \Rightarrow a = b$.

Demonstração. Por hipóteses, $\begin{cases} a \mid b \overset{\text{Def.6}}{\Rightarrow} \exists\ p \in \mathbb{Z} \text{ tal que } b = a \cdot p\ (i) \\ b \mid a \overset{\text{Def.6}}{\Rightarrow} \exists\ q \in \mathbb{Z} \text{ tal que } a = b \cdot q\ (ii) \end{cases}$

Assim, como $a = b \cdot q \overset{(i)}{\Rightarrow} a = (ap) \cdot q \overset{associativa}{=} a \cdot (pq) \Rightarrow pq$ é elemento neutro multiplicativo.

Logo, $p \cdot q = 1$, com $p, q \in \mathbb{Z} \Rightarrow \begin{cases} p = q = 1 \overset{(i)}{\Rightarrow} a = b \\ p = q = -1 \overset{(i)}{\Rightarrow} a = -b \end{cases}$

Note que, como $a, b \in \mathbb{N} \cup \{0\}$, $a = -b$ só é válida se $a = b = 0$. Isso ocorre porque os números naturais ($\mathbb{N}$) não incluem números negativos. Se a e b são números naturais, então $-b$ não pode ser um número natural. Consequentemente, a igualdade $a = -b$ é impossível para $a, b \in \mathbb{N}$. Portanto, a única solução possível para $a = -b$ quando $a, b \in \mathbb{N} \cup \{0\}$ é $a = b = 0$.

■

Proposição 13. Sejam $a, b \in \mathbb{Z}$, se $ab = 1 \Rightarrow a = b = 1$ ou $a = b = -1$.

Demonstração. Note que $a \neq 0$ e $b \neq 0$, pois se $a = 0$ ou $b = 0 \Rightarrow a \cdot b = 0$ (Além disso, $\mathbb{Z}$ é um domínio de integridade).

Logo, $1 \leq \mid a \mid$ e $1 \leq \mid b \mid$, pois $\nexists n \in \mathbb{Z}$ tal que $0 < n < 1$ ou $-1 < n < 0$.

Assim, $1 \leq \mid a \mid \leq \mid a \mid \cdot \mid b \mid = \mid a \cdot b \mid = \mid 1 \mid = 1 \Rightarrow \mid a \mid = 1 \Rightarrow a = 1$ ou $a = -1$ (Propriedades de módulo). Sendo assim, têm-se dois casos para analisar:

Se $\begin{cases} a = 1, ab = 1 \Rightarrow 1 \cdot b = 1 \overset{elemento\ neutro}{\Rightarrow} b = 1. \\ a = -1, ab = 1 \Rightarrow -b = 1 \Rightarrow -b + (b-1) = 1 + (b-1) \overset{elemento\ simétrico}{\Rightarrow} -1 = b. \end{cases}$

$\therefore$ se $ab = 1 \Rightarrow a = b = 1$ ou $a = b = -1$.

■

Proposição 14. $\forall a, b, c, d \in \mathbb{Z}$, se $a \mid b$ e $c \mid d \Rightarrow ac \mid bd$.

Demonstração. Por hipóteses, $\begin{cases} a \mid b \overset{\text{Def.6}}{\Rightarrow} \exists\ p \in \mathbb{Z} \text{ tal que } b = a \cdot p\ (i) \\ c \mid d \overset{\text{Def.6}}{\Rightarrow} \exists\ q \in \mathbb{Z} \text{ tal que } d = c \cdot q\ (ii) \end{cases}$

Com o produto de *(i)* e *(ii)* obtêm-se: $bd = (ap) \cdot (cq) \overset{associativa}{=} (ac) \cdot (pq) \overset{fechamento}{=} ac \cdot k$, com $k = pq$.

Logo, $bd = ac \cdot k$ $(k \in \mathbb{Z})$.

$\therefore ac \mid bd$.

■

Proposição 15. Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então $a \mid b \Leftrightarrow a \mid c$.

Demonstração. $(\Rightarrow)$ Por hipóteses, $\begin{cases} a \mid (b+c) \overset{\text{Def.6}}{\Rightarrow} \exists\ p \in \mathbb{Z} \text{ tal que } (b+c) = a \cdot p\ (i) \\ a \mid b \overset{\text{Def.6}}{\Rightarrow} \exists\ q \in \mathbb{Z} \text{ tal que } b = a \cdot q\ (ii) \end{cases}$

Substituindo *(ii)* em *(i)*, tem-se: $(aq) + c = ap \Rightarrow c = ap - aq \overset{distributiva}{=} a(p-q) = a \cdot k$, com $k = p - q$. Logo $c = ak$ $(k \in \mathbb{Z})$.

$\therefore a \mid c$.

$(\Leftarrow)$ Para a recíproca é análogo.

Por hipóteses, $\begin{cases} a \mid (b+c) \overset{\text{Def.6}}{\Rightarrow} \exists\ p \in \mathbb{Z} \text{ tal que } (b+c) = a \cdot p\ (i) \\ a \mid c \overset{\text{Def.6}}{\Rightarrow} \exists\ q \in \mathbb{Z} \text{ tal que } c = a \cdot q\ (ii) \end{cases}$

Substituindo *(ii)* em *(i)*, tem-se: $b + (aq) = ap \Rightarrow b = ap - aq \overset{distributiva}{=} a(p-q) = a \cdot k$, com $k = p - q$. Logo $b = ak$ $(k \in \mathbb{Z})$.

$\therefore a \mid b$.

■

Proposição 16. Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então para todo $x, y \in \mathbb{Z}$ tem-se $a \mid (bx + cy)$.

Demonstração. Por hipóteses, $\begin{cases} a \mid b \overset{\text{Def.6}}{\Rightarrow} \exists\ p \in \mathbb{Z} \text{ tal que } b = a \cdot p\ (i) \\ a \mid c \overset{\text{Def.6}}{\Rightarrow} \exists\ q \in \mathbb{Z} \text{ tal que } c = a \cdot q\ (ii) \end{cases}$

Logo $bx + cy \overset{(i)\ e\ (ii)}{=} (ap)x + (aq)y \overset{associativa}{=} a(px) + a(qy) \overset{distributiva}{=} a(px + qy) = a \cdot k$, com $k = px + qy$. Logo $bx + cy = ak$ $(k \in \mathbb{Z})$.

$\therefore a \mid (bx + cy)$. ■

A *divisibilidade* ocorre quando uma número é múltiplo de outro, ou seja, quando a divisão entre eles resulta em resto zero. Por outro lado, a *Divisão Euclidiana* garante que, dados dois números inteiros, pode-se expressar um deles como um múltiplo do outro mais um resto menor. Assim, a divisão euclidiana torna-se uma ferramenta fundamental para complementar o processo de divisibilidade, possibilitando explorar as relações de divisibilidade de forma sistemática.

2.4.1 Divisão Euclidiana

EUCLIDES em sua obra "*Os Elementos*", traduzida por Irineu Bicudo em 2009, apresenta a *Divisão Euclidiana* de forma implícita quando trabalha no Livro V (Teoria das Proporções) com conceitos como razão, proporção e proporcionalidade. No Livro VII (Teoria dos Números) apresenta conceitos como divisibilidade, máximo divisor comum e mínimo divisor comum. Por fim, no Livro X (Incomensuráveis) aborda números irracionais e proporcionalidades entre eles, para analisar limitações em casos específicos.

Portanto, em seu livro, Euclides não apresenta a divisão euclidiana de forma explícita. De acordo com Hefez (2022, p. 36), Euclides "utiliza, sem enunciá-lo explicitamente, o fato de que é sempre possível efetuar uma divisão de a por b, com resto (Euclides trabalhava apenas com números naturais)". Ainda assim, Euclides, apesar de não formalizar a divisão euclidiana, contribuiu de forma significativa com conceitos e ferramentas matemáticas que fundamentam esse algoritmo.

Teorema 4. *(Divisão Euclidiana) Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que $a = bq + r$, com $0 \leq r < \mid b \mid$.*

Note que, na divisão euclidiana, o resto da divisão de a por b é zero se, e somente se, b divide a. Em relação a demonstração do Teorema acima, pode-se encontrar na página 37 do livro de Aritmética de Abramo Hefez (2022).

Exemplo 3. *Mostre, para todo $a \in \mathbb{Z}$, que $2 \mid (a^2 - a)$.*

Demonstração. Note que $a^2 - a = a(a-1)$. Além disso, pelo algoritmo de Euclides, pode-se escrever: $a = 2k + r$, $k \in \mathbb{Z}$ e $r \in \{0, 1\}$. Assim, precisa-se analisar duas possibilidades:

(i) a é par: $a = 2k \Rightarrow a(a-1) = 2k(2k-1) = (2k)^2 - (2k) \Rightarrow 2 \mid (a^2 - a)$.

(ii) a é impar: $a = 2k + 1 \Rightarrow a(a-1) = (2k+1)[(2k+1) - 1] = (2k+1)(2k) \overset{\text{Distrib.}}{=} 2(2k^2 + k) = 2k'$, com $2k^2 + k = k' \Rightarrow a(a-1) = 2k' \overset{\text{Def.6}}{\Rightarrow} 2 \mid a(a-1)$.

Portanto, em ambos os casos $2 \mid (a^2 - a)$.

■

Corolário 1. Se p é um número primo e a é um número natural não divisível por p ($p \nmid a$), então $p \mid a^{p-1} - 1$.

Demonstração: Hefez (2022, p. 106).

2.4.2 Algoritmo de Euclides

O algoritmo de Euclides é um método prático para encontrar o Máximo Divisor Comum (MDC) de dois números inteiros diferentes de zero. Neste método utiliza-se do processo das divisões sucessivas. Vale enfatizar que o MDC é útil para dividir, agrupar e distribuir da melhor forma possível pessoas, objetos ou recursos.

Exemplo 4. Calcular o mdc entre 637 e 3887 pelo método das divisões sucessivas.

	6	9	1	4
3887	637	65	52	13
65	52	13	0	

Na primeira linha, estão os quocientes das divisões realizadas. Na linha seguinte, aparecem os divisores e dividendos das divisões efetuadas. E, na terceira linha, estão os restos das divisões realizadas. Assim, o MDC é o último resto não nulo do processo das divisões sucessivas.

Note que, no exemplo acima, o Algoritmo de Euclides fornece:

(i) $3887 = 637 \cdot 6 + 65 \Rightarrow 65 = 3887 - 637 \cdot 6$;

(ii) $637 = 65 \cdot 9 + 52 \Rightarrow 52 = 637 - 65 \cdot 9$;

(iii) $65 = 52 \cdot 1 + 13 \Rightarrow 13 = 65 - 52 \cdot 1$;

(iv) $52 = 13 \cdot 4 + 0$.

Portanto, o $mdc\ (637, 3887) = 13$.

A partir do $mdc\ (637, 3887)$, pode-se determinar números inteiros m e n tal que $(a, b) = ma + nb$, em que $a = 637$ e $b = 3887$. Para isso, é necessário utilizar o Algoritmo de Euclides de trás para frente:

$$\begin{aligned}
13 &= 65 - 52 \cdot 1 \\
&\overset{(ii)}{=} 65 - 1(637 - 65 \cdot 9) \\
&= 65 \cdot 1 + 65 \cdot 9 - 1 \cdot 637 \\
&= 65 \cdot 10 - 1 \cdot 637 \\
&\overset{(i)}{=} (3887 - 637 \cdot 6) \cdot 10 - 1 \cdot 637 \\
&= 3887 \cdot 10 - 60 \cdot 637 - 1 \cdot 637 \\
&= 637 \cdot (-61) + 3887 \cdot (10) \Rightarrow m = -61 \text{ e } n = 10.
\end{aligned}$$

$\therefore (637, 3887) = (-61) \cdot 637 + (10) \cdot 3887.$

2.4.3 Máximo Divisor Comum

Sabe-se que o Máximo Divisor Comum (MDC) é o maior número que divide dois ou mais números simultaneamente.

Definição 7. *(Divisor Comum) Sejam $a, b \in \mathbb{Z}$, distintos ou não. Diz-se que d é um divisor comum de a e b se $d \mid a$ e $d \mid b$.*

Exemplo 5. *Os números* 30 *e* 24 *possuem os seguintes divisores comuns:* ± 1, ± 2, ± 3 *e* ± 6.

Definição 8. *(Máximo Divisor Comum) Sejam a e b inteiros diferentes de zero. O máximo divisor comum (MDC) de a e b é o número inteiro d, que satisfaz as seguintes propriedades:*

(i) *d é um divisor comum de a e b, isto é, $d \mid a$ e $d \mid b$.*

(ii) *d é o maior inteiro positivo com a propriedade (i).*

Notação 2. *Denota-se por $d = mdc\ (a, b)$ ou por $d = (a, b)$ o MDC entre a e b.*

Note que dados $a, b \in \mathbb{Z}$ não ambos nulos, se existir o $mdc\ (a, b)$ de a e b, então $(a, b) = (-a, b) = (a, -b) = (-a, -b)$. Assim, para o cálculo envolvendo o mdc de dois números, pode-se sempre supô-los como positivos. Além disso, como o mdc de a e b não depende da ordem em que a e b são tomados, tem-se que $(a, b) = (b, a)$.

Lema 1. *(Lema de Euclides) Sejam $a, b, n \in \mathbb{Z}$. Se existir $(a, b - na)$, então, (a, b) existe e $(a, b) = (a, b - na)$.*

Demonstração. Seja $d = (a, b - na) \overset{\text{Def.7}}{\Rightarrow} d \mid a$ e $d \mid (b - na)$. Assim, como $d \mid a \Rightarrow d \mid a \cdot n$. Assim, se $d \mid (b - na)$ e $d \mid na \Rightarrow d \mid b - na + na \Rightarrow d \mid b$.

Agora, suponha que c seja um divisor comum de a e $b \overset{\text{Def.7}}{\Rightarrow} c \mid a$ e $c \mid b$. Assim, como $c \mid a \Rightarrow c \mid na$. Logo, $c \mid (b \cdot 1) + (-1) \cdot na = b - na$. Consequentemente, como $c \mid a$ e $c \mid b - na \Rightarrow c \mid (a, b - na) = d \Rightarrow c \mid d$. Isso prova que $d = (a, b)$.

■

Corolário 2. *Quaisquer que sejam $a, b \in \mathbb{Z}$, não ambos nulos, e $n \in \mathbb{N}$, tem-se que $(na, nb) = n(a, b)$.*

Proposição 17. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

As demonstrações do Corolário 2 e da Proposição 17, podem ser encontradas nas páginas 63 e 64 do livro de Aritmética de HEFEZ (2022).

A divisibilidade de um número consiste em verificar se esse número é divisível por outro (ou se é múltiplo do outro), este processo realizado a partir de sucessivas divisões para decompor um número em seus fatores primos é chamado de *fatoração*. O *Teorema Fundamental da Aritmética*, por exemplo, afirma que todo número inteiro maior que 1 pode ser escrito de forma única como um produto de números primos, obtida a partir dessas sucessivas divisões por números primos, demonstrando a importância dos *números primos* na estrutura dos números inteiros.

2.5 Números primos

Definição 9. *Diz-se que um número natural p é primo se, e somente se, satisfaz as seguintes condições:*

(i) $p \neq 0$ e $p \neq 1$;

(ii) Os únicos divisores de p são 1 e p.

Se p não é primo, então p é dito composto.
Se o mdc $(a, b) = 1$, então diz-se que a e b são primos entre si ou co-primos.

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da Definição 9 os seguintes fatos:

(i) Se $p \mid q$, então $p = q$.

Demonstração. Por hipótese $p \mid q$, mas p é primo. Assim, tem-se $p = 1$ ou $p = q$. No entanto, p também é primo $\Rightarrow p \geq 2$. Logo $p = q$.

$\therefore$ Se $p \mid q$, então $p = q$. ■

(ii) Se $p \nmid a$, então $(p, a) = 1$.

Demonstração. Suponha que $(p, a) = d$. Assim, tem-se que $d \mid p$ e $d \mid a$. Como p é primo e $d \mid p \Rightarrow d = 1$ ou $d = p$.

Se $d = p \Rightarrow p \mid a$. Absurdo por hipótese. Logo $d = 1$.

$\therefore$ Se $p \nmid a$, então $(p, a) = 1$. ■

Proposição 18. *(Lema de Euclides) Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Suponha que $p \nmid a$ (sem perda de generalidade). Se $p \nmid a \Rightarrow (p, a) = 1$. Logo, $\exists x_0, y_0 \in \mathbb{Z}$ tal que $x_0 \cdot p + y_0 \cdot a = 1 \overset{\cdot b}{\Rightarrow} p(x_0 b) + y_0(ab) = b$. Como $p \mid p$ e $p \mid ab \Rightarrow p$ divide a combinação linear de p e ab. Portanto, $p \mid b$.

■

Corolário 3. *Se $p, p_1, \ldots, p_n$ são números primos e, se $p \mid p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, \ldots, n$.*

Em relação a quantidade de Números Primos: quantos existem?

Teorema 5. *Existem infinitos números primos.*

Lema 2. *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.*

Lema 3. *(Lema de Gauss) Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Lema 4. *Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < 1 < p$, são todos divisíveis por p.*

Demonstração. A demonstração será por indução matemática em i.

(i) Para $i = 1$: $\binom{p}{1} = \dfrac{p!}{1!(p-1)!} = \dfrac{p(p-1)!}{1(p-1)!} = p$, e como $p \mid p$, isso sugere que o lema é válido para $i = 1$.

(ii) Suponha que o lema seja válido para $i > 1$, ou seja, $1 < i < p$.

Sabe-se que $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-(i-1))}{i!}$ (1).

Por hipótese, p é primo e $i < p$, então o MDC$(i!, p) = 1$, pois $i!$ não possui fator primo maior do que ele mesmo na sua decomposição. Logo, $i! \nmid p$.

Desse modo, pelo Lema de Gauss, tem-se que $i! \mid (p-1)\cdots(p-(i-1))$. Assim, como $i! \mid (p-1)\cdots(p-(i-1)) \overset{\text{Def.6}}{\Rightarrow} \exists k \in \mathbb{N}$ tal que $(p-1)\cdots(p-(i-1)) = k \cdot i!$ (2). Substituindo a parte (2) em (1), obtém-se: $\binom{p}{i} = \frac{p(k \cdot i!)}{i!} = pk \Rightarrow \binom{p}{i} = pk \overset{\text{Def.6}}{\Rightarrow} p \mid \binom{p}{i}$. Logo, se p é primo, os números $\binom{p}{i}$, onde $0 < 1 < p$, são todos divisíveis por p.

■

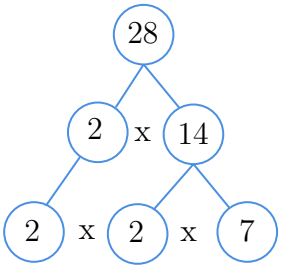
Para realizar o processo de fatoração de um número é necessário utilizar o método de divisões sucessivas a partir de números primos. Desse modo, escreve-se os números compostos a partir de produto de seus fatores primos.

2.5.1 Fatoração

Na matemática, a fatoração se apresenta como um processo fundamental para desvendar a composição de números e expressões. Através dela, é possível decompor um número ou expressão em seus "blocos de construção"básicos, os chamados fatores. Esses fatores, por sua vez, são sempre compostos por números primos, o que caracteriza a decomposição em fatores primos.

Na Educação Básica das Escolas brasileiras, aprende-se a decomposição em fatores primos através de divisões sucessivas para, posteriormente, ensinar-se o processo de fatoração de expressões algébricas. Veja os exemplos a seguir:

Exemplo 6. Decomposição em fatores primos do número 28 a partir de divisões sucessivas:



Fonte: Elaborado pelo autor, 2024.

Exemplo 7. Decomposição em fatores primos, através de divisões por números primos:

	180	2	
	90	2	
Quocientes	45	3	Divisores primos
	15	3	
	5	5	
	1	$180 = 2^2 \cdot 3^2 \cdot 5$	

Fonte: Elaborado pelo autor, 2024.

Exemplo 8. (Fator comum em evidência) Fatore a expressão $5x + 5y$.

Note que os monômios da expressão acima possuem um fator em comum, o coeficiente 5. Assim, para fatorar a expressão, basta por esse fator comum em evidência: $5(x + y)$.

Exemplo 9. (Agrupamento de termos semelhantes) Fatore a expressão $2ax + 3x + 4y + 5yb$.

Observe que a expressão acima não possui um fator comum, mas é possível agrupá-los a partir dos termos com parte literal semelhantes: $x(2a + 3) + y(4 + 5b)$.

Como visto até aqui, a fatoração pode ser realizada em números e expressões, nos números a partir da decomposição em fatores primos. Já nas expressões algébricas, a partir de um ou mais fatores em comum em evidência ou a partir do agrupamento de termos semelhantes com base na sua parte literal. Além destes citados, foram desenvolvidos os produtos notáveis para encontrar a decomposição de uma expressão algébrica. Entre eles tem-se o quadrado da soma e da diferença e o cubo da soma e da diferença.

Teorema 6. *(Teorema Fundamental da Aritmética) Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Outro Teorema bastante importante que aborda essa forma de escrever de modo único uma fatoração é o Teorema da Fatoração Única. Nele cada número inteiro maior que 1 possui uma única decomposição em fatores primos, ou seja, apenas uma maneira de expressá-lo como o produto de números primos.

Teorema 7. *(Teorema Fundamental da Aritmética) Um inteiro positivo $n \geq 2$ pode ser escrito, de modo único, na forma $n = p_1^{e_1} \cdots p_k^{e_k}$, em que $1 < p_1 < p_2 < p_3 < \cdots < p_k$ são números primos e $e_1, \ldots, e_k$ são inteiros positivos.*

De acordo com Coutinho (2023, p. 38), "os expoentes $e_1, \ldots, e_k$ no teorema acima são chamados de *multiplicidades*. Assim, a multiplicidade de p_1 na fatoração de n é e_1. Em outras palavras, a *multiplicidade* de p_1 é o maior expoente e_1 tal que $p_1^{e_1}$ divide n". Além disso, note que n tem k fatores primos distintos e que a quantidade total de fatores primos, distintos ou não, é a soma das multiplicidades $e_1, \ldots, e_k$.

2.5.2 Fatoração de Fermat

O algoritmo de fatoração visto anteriormente é bastante útil para decomposição de um número quando o termo que se quer fatorar é divisível por um primo pequeno, como o

$2, 3, 5, 7$, ou o 11, por exemplo. No entanto, para um computador o quão pequeno é esse primo depende do seu nível de processamento. Por exemplo, o supercomputador da USP, Cluster Euler, para um primo p de 47 algarismos, levaria, pelo algoritmo tradicional de fatoração, aproximadamente, $4,348 \cdot 10^7$ *segundos*, que corresponde a mais de 1 ano e 4 meses realizando os testes de divisões (OBMEP, 2020).

Segundo Carneiro (2017, p. 43), a Fatoração de Fermat inicia-se "supondo que n é ímpar, porque se n fosse par, então 2 é um de seus fatores. A ideia é tentar determinar números inteiros positivos x e y tais que $n = x^2 - y^2$."

Note que $x^2 - y^2 = (x + y) \cdot (x - y) \Rightarrow n = x^2 - y^2 = (x + y) \cdot (x - y)$.

Logo, $x - y$ e $x + y$ são fatores de n.

Para conseguir utilizar o algoritmo de Fermat, precisa-se de um computador com um algoritmo que consiga determinar a $\sqrt{n}$. Assim, suponha que esse computador esteja a disposição para realização desse processo. De acordo com Coutinho (2023, p. 41), "é suficiente obter a parte inteira da raiz quadrada de n."Isto ocorre porque um dos fatores, no caso $(x - y)$, é menor ou igual a $\sqrt{n}$.

Do mesmo modo, CARNEIRO complementa COUTINHO dizendo que "x é incrementado de um a um, até que seja encontrado um valor inteiro para $y = \sqrt{x^2 - n}$, então são encontrados os valores dos fatores $(x + y)$ e $(x - y)$."Consequentemente, se o valor inteiro para y não é encontrado, o número é primo, e o algoritmo, para este caso, é finalizado para $x = \dfrac{(n + 1)}{2}$.

Notação 3. Seja $r \in \mathbb{R}$, sua parte inteira será denotada por [r]. É claro que, se r é inteiro, então $[r] = r$.

Exemplo 10. $[\sqrt{125}] = 11$ e $[\pi] = 3$.

Exemplo 11. Fatore o número $n = 32.881$ usando o algoritmo de Fermat.

Como $\sqrt{32.881} = 181,331... \Rightarrow [181, 331 \dots] = 181$. Assim, deve-se iniciar o incremento de um em um a partir do valor $181 + 1 = 182$. Logo, os fatores são:

Tabela 2.1: Algoritmo de Fermat

x	$y = \sqrt{x^2 - n}$
182	$15,588\ldots$
183	$24,657\ldots$
184	$31,224\ldots$
185	$36,660\ldots$
186	$41,412\ldots$
187	$45,694\ldots$
188	$49,628\ldots$
189	$53,291\ldots$
190	$56,736\ldots$
191	60

Fonte: CARNEIRO, 2017, p. 45.

Desse modo, tem-se: $x = 191$ e $y = 60 \Rightarrow x+y = 191+60 = 251$ e $x-y = 191-60 = 131$. Portanto, $(x + y) = 251$ e $(x - y) = 131 \Rightarrow 32.881 = 251 \cdot 131$.

Exemplo 12. Fatore o número $n = 527$ usando o algoritmo de Fermat.

Como $\sqrt{527} = 22,956... \Rightarrow [22,956\ldots] = 22$. Assim, deve-se iniciar o incremento de um em um a partir do valor $22 + 1 = 23$. Logo, os fatores são:

Tabela 2.2: Algoritmo de Fermat - Resolução

x	$y = \sqrt{x^2 - n}$
23	$1,414\ldots$
24	7

Fonte: Elaborado pelo autor, 2024.

Desse modo, tem-se: $x = 24$ e $y = 7 \Rightarrow x + y = 24 + 7 = 31$ e $x - y = 24 - 7 = 17$. Portanto, $(x + y) = 31$ e $(x - y) = 17 \Rightarrow 527 = 31 \cdot 17$.

A demonstração do algoritmo de Fermat pode ser encontrada no livro *Números Inteiros e Criptografia RSA* de Coutinho (2023) nas páginas 42 e 43.

Os números primos, a fatoração e a aritmética dos restos estão intimamente ligados. Ao analisar os restos das divisões por números primos, a *aritmética dos restos* possibilita identificar os possíveis divisores primos de um número, reduzindo o número de divisões necessárias no processo de fatoração. Essa relação é fundamental para diversas aplicações, como na criptografia, em que a compreensão da divisibilidade dos números é essencial.

2.6 Aritmética dos Restos

A aritmética dos restos, também conhecida como aritmética modular, é um ramo da matemática que explora os restos da divisão de dois números inteiros por um outro

número específico. Além disso, quando números diferentes possuem o mesmo resto quando divididos por um mesmo número específico (chamado de módulo), denominamos este processo de *Congruência Modular*.

Exemplo 13. Suponha que você tenha em sua casa um relógio analógico de parede, aqueles com apenas 12 horas para realizar as marcações de hora. Ao somar 7 horas, o relógio ultrapassa o limite de 12 horas disponíveis e retorna às 7h. Na aritmética modular, essa ideia se aplica da seguinte forma: 12h + 7h = 19 horas, quando divide-se 19h pelas 12 horas, obtêm-se 1h de quociente e 7 de resto (19h = 12h x 1 + 7h). Ou seja, 19h é congruente a 7h módulo 12h.

Definição 10. Sejam $m \in \mathbb{N}$ e $a, b \in \mathbb{Z}$. Diz-se que a e b são congruentes módulo m se os restos de sua divisão por m são iguais. Assim,

Notação 4. Se os inteiros a e b são congruentes módulo m, escreve-se:

$$\boxed{a \equiv b \ mod \ m}.$$

Notação 5. Se os inteiros a e b não são congruentes módulo m, escreve-se:

$$\boxed{a \not\equiv b \ mod \ m}.$$

Sabe-se que o resto da divisão de qualquer número inteiro por 1 é sempre zero. Isso acarreta em inteiros módulo 1 sempre com o mesmo resto, ou seja, sempre congruentes. Portanto, trata-se de uma situação desinteressante para o tópico Aritmética dos Restos, pois é um caso óbvio. Em virtude disso, considere sempre $m > 1$.

Segundo Hefez (2022, p. 130), "para verificar se dois números inteiros são congruentes módulo m, não é necessário efetuar a divisão euclidiana de ambos por m para depois comparar os restos". O artifício para isso é a proposição a seguir:

Proposição 19. Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \ mod \ m$ se, e somente se, $m \mid (b - a)$.

Demonstração. ($\Rightarrow$) Por hipótese, $a \equiv b \ mod \ m$. Assim, pode-se escrever a e b como:

$$\begin{cases} a = mq_1 + r_1 \ \textit{tal que} \ q_1, r_1 \in \mathbb{Z}, 0 \leq r_1 < m \ \textit{(Como } m > 1 \ \textit{não precisa do módulo).} \\ b = mq_2 + r_2 \ \textit{tal que} \ q_2, r_2 \in \mathbb{Z}, 0 \leq r_2 < m \ \textit{(} m > 1\textit{).} \end{cases}$$

Pela definição de congruência (Def. 10), como $a \equiv b \ mod \ m \Rightarrow r_1 = r_2$. Desse modo, realizando a diferença entre b e a, obtém-se:

$$\begin{aligned} b - a &= (mq_2 + r) - (mq_1 + r) & \\ &= mq_2 + r - mq_1 - r & \text{(Elemento simétrico)} \\ &= mq_2 - mq_1 & \text{(Propriedade distributiva)} \\ &= m(q_2 - q_1) & \end{aligned}$$

Como $b - a = m(q_2 - q_1) \overset{\text{Def.6}}{\Rightarrow} m \mid b - a$.

($\Leftarrow$) Por hipótese, $m \mid b-a \overset{\text{Def.6}}{\Rightarrow} \exists c \in \mathbb{Z}$ tal que $b-a = m \cdot c \Rightarrow b = mc + a$. Agora, seja r o resto da divisão de a por m. Assim, pela *Divisão Euclidiana*, tem-se: $a = mq + r$, com $q \in \mathbb{Z}$ e $0 \leq r < m$.

Como $b = mc+a \Rightarrow b = mc+(mq+r) \overset{\text{associativa}}{=} (mc+mq)+r \overset{\text{distributiva}}{=} m(c+q)+r \Rightarrow b = m(c+q)+r$. Sabe-se que $0 \leq r < m$, consequentemente, pela unicidade do resto e do quociente de uma divisão, concluí-se que $c+q$ é o quociente da divisão de b por m e r é o resto da divisão de b por m. Logo os inteiros a e b possuem o mesmo resto quando divididos por m.

$\therefore a \equiv b \ mod \ m$.

■

Em consequência da Definição 10 sobre congruências, decorre as seguintes relações de equivalência:

Proposição 20. Seja $m \in \mathbb{N}$, $\forall \ a, b, c \in \mathbb{Z}$, tem-se que:

(i) $a \equiv a \ mod \ m$ *(Propriedade Reflexiva)*,

(ii) se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$ *(Propriedade Simétrica)*,

(iii) se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$, então $a \equiv c \ mod \ m$ *(Propriedade Transitiva)*.

Demonstração. Observe as demonstrações das propriedades elencadas acima:

(i) Pela Proposição 19: Para $a, b, m \in \mathbb{Z}$, com $m > 1$, tem-se que $a \equiv b \ mod \ m \Leftrightarrow m \mid b-a$. Sendo assim, como $m \cdot 0 = 0$ e $a - a = 0 \Rightarrow m \mid (a-a) \Leftrightarrow a \equiv a \ mod \ m$.

(ii) Por hipótese, $a \equiv b \ mod \ m \overset{\text{Prop.19}}{\Leftrightarrow} m \mid b-a \overset{\text{Def.6}}{\Rightarrow} \exists \ k \in \mathbb{Z}$ tal que $b - a = mk$. Assim, como $b-a = -(a-b) = -(mk) = (-k)m$, com $-k \in \mathbb{Z} \Rightarrow m \mid (a-b)$. Logo $b \equiv a \ mod \ m$.

(iii) Por hipóteses, $\begin{cases} a \equiv b \ mod \ m \overset{\text{Prop. 19}}{\Leftrightarrow} m \mid (b-a) \Rightarrow \exists p \in \mathbb{Z} \ tal \ que \ b - a = mp. \\ b \equiv c \ mod \ m \overset{\text{Prop. 19}}{\Leftrightarrow} m \mid (c-b) \Rightarrow \exists q \in \mathbb{Z} \ tal \ que \ c - b = mq. \end{cases}$

Sabe-se que $(b-a) = mp$ e $(c-b) = mq$. Assim, realizando a soma entre as duas equações, obtém-se: $c - a = mp + mq \overset{\text{dist.}}{\Rightarrow} c - a = m(p+q) \overset{\text{Def.6}}{\Leftrightarrow} m \mid (c-a)$.

Logo $a \equiv c \ mod \ m$.

■

Proposição 21. *Sejam* $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.

(i) *Se* $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, *então* $a + c \equiv b + d \ mod \ m$.

(ii) *Se* $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, *então* $ac \equiv bd \ mod \ m$.

Demonstração. Observe as demonstrações da parte (i) e (ii) da proposição acima:

(i) Por hipóteses, $\begin{cases} a \equiv b \ mod \ m \overset{\text{Prop.19}}{\Leftrightarrow} \ m \mid (b-a) \overset{\text{Def.6}}{\Rightarrow} \ \exists p \in \mathbb{Z} \mid b-a = mp. \\ c \equiv d \ mod \ m \overset{\text{Prop.19}}{\Leftrightarrow} \ m \mid (d-c) \overset{\text{Def.6}}{\Rightarrow} \ \exists q \in \mathbb{Z} \mid d-c = mq. \end{cases}$

Realizando a soma das equações obtidas, tem-se: $b+d-a-c = mp+mq \overset{\text{dist.}}{\Rightarrow}$ $(b+d)-(a+c) = m(p+q)$. Logo $m \mid (b+d)-(a+c) \overset{\text{Prop.19}}{\Leftrightarrow} \ a+c \equiv b+d \ mod \ m$.

$\therefore$ *Se* $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$ *, então* $a+c \equiv b+d \ mod \ m$.

(ii) ($\Rightarrow$) Por hipóteses, $\begin{cases} a \equiv b \ mod \ m \overset{\text{Prop.19}}{\Leftrightarrow} \ m \mid (b-a) \overset{\text{Def.6}}{\Rightarrow} \ \exists p \in \mathbb{Z} \mid b-a = mp. \\ c \equiv d \ mod \ m \overset{\text{Prop.19}}{\Leftrightarrow} \ m \mid (d-c) \overset{\text{Def.6}}{\Rightarrow} \ \exists q \in \mathbb{Z} \mid d-c = mq. \end{cases}$

Multiplicando a primeira equação por c e a segunda por b, obtém-se:

$\begin{cases} b-a = mp \overset{\cdot c}{\Rightarrow} \ c(b-a) = c(mp) \overset{\text{dist. e assoc.}}{\Rightarrow} \ bc-ac = (cp)m \\ d-c = mq \overset{\cdot b}{\Rightarrow} \ b(d-c) = b(mq) \overset{\text{dist. e assoc.}}{\Rightarrow} \ bd-bc = (bq)m \end{cases}$

Se $m \mid (b-a)$ e $m \mid (d-c)$, então m divide a combinação linear. Assim, pela soma das equações obtidas acima, tem-se:

$$\begin{array}{rcll} bc-ac+bd-bc & = & (cp)m+(bq)m & \text{(Distributiva e Elemento simétrico)} \\ bd-ac & = & (cp+bq)m & \text{(Propriedade Distributiva)} \\ bd-ac & = & km & \text{(Tomando } k = cp+bq, \text{ com } k \in \mathbb{Z}) \end{array}$$

Como $bd-ac = km \overset{\text{Def.6}}{\Rightarrow} \ m \mid (bd-ac) \overset{\text{Prop.19}}{\Leftrightarrow} \ ac \equiv bd \ mod \ m$.

$\therefore$ *Se* $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$ *, então* $ac \equiv bd \ mod \ m$.

■

Corolário 4. Para todos $n \in \mathbb{N}$, $a, b, m \in \mathbb{Z}$, com $m > 1$. Se $a \equiv b \ mod \ m$, então tem-se que $a^n \equiv b^n \ mod \ m$.

A demonstração do Corolário acima é feita por indução matemática fraca em n e encontra-se na página 131 do livro de Hefez (2022). Já o Teorema abaixo, pode-se encontrar a demonstração nas páginas 63 e 64 do livro de Carneiro (2017).

Teorema 8. (Pequeno Teorema de Fermat) Sejam $a \in \mathbb{Z}$ e p um número primo tal que $p \nmid a$, então $a^{p-1} \equiv 1 \ mod \ p$.

Exemplo 14. Ache o resto da divisão de 2^{100} por 11.

Resolução: Como $11 \nmid 2$, pode-se utilizar o Pequeno Teorema de Fermat (Teorema 8): $a^{p-1} \equiv 1 \ mod \ p$. Assim, tem-se:

$2^{10} \equiv 1 \ mod \ 11 \overset{\wedge 10}{\Rightarrow} \ (2^{10})^{10} \equiv (1)^{10} \ mod \ 11 \Rightarrow 2^{100} \equiv 1 \ mod \ 11 \Rightarrow \boxed{resto = 1}$.

Exemplo 15. Determine o resto da divisão de 3^{100} por 7.

Resolução: Como $7 \nmid 3$, pode-se utilizar o Pequeno Teorema de Fermat (Teorema 8): $a^{p-1} \equiv 1 \ mod \ p$. Assim, tem-se: $3^6 \equiv 1 \ mod \ 7$. Além disso, como $100 = 6 \cdot 16 + 4$, é

possível usar esse fato em ambos os lados da congruência para chegar-se no expoente 100, obtendo-se: $(3^6)^{16} \cdot 3^4 \equiv (1)^{16} \cdot 3^4 \ mod\ 7 \Rightarrow 3^{100} \equiv 3^4 \ mod\ 7$ (i).

Como $3^4 = 81 \equiv 4 \ mod\ 7$ (ii), então, por transitividade de (i) e (ii), segue-se que: $3^{100} \equiv 4 \ mod\ 7 \Rightarrow \boxed{\text{resto} = 4}$.

Logo, o resto da divisão de 3^{100} por 7 é 4.

Exemplo 16. Ache o resto da divisão de $(116 + 17^{17})^{21}$ por 8.

Note que p não é primo, então precisa-se utilizasse de outras estratégias.

Resolução: Como $\begin{cases} 116 = 14 \cdot 8 + 4 \Rightarrow 116 \equiv 4 \ mod\ 8 \text{ (i)} \\ 17 = 2 \cdot 8 + 1 \Rightarrow 17 \equiv 1 \ mod\ 8 \overset{\wedge 17}{\Rightarrow} \ 17^{17} \equiv 1 \ mod\ 8 \text{ (ii)} \end{cases}$

Agora, com a soma entre as partes (i) e (ii), obtém-se: $116 + 17^{17} \equiv 5 \ mod\ 8 \overset{\wedge 21}{\Rightarrow} (116 + 17^{17})^{21} \equiv 5^{21} \ mod\ 8$ (iii).

Note que $5^2 \equiv 1 \ mod\ 8 \overset{\wedge 10}{\Rightarrow} \ (5^2)^{10} \equiv 1^{10} \ mod\ 8 \Rightarrow 5^{20} \equiv 1 \ mod\ 8$ (iv).

Desse modo, utilizando o fato de $5 \equiv 5 \ mod\ 8$ (v), pelo produto de (iv) e (v), obtém-se: $5^{21} \equiv 5 \ mod\ 8$ (vi) $\Rightarrow \boxed{\text{resto} = 5}$.

Como consequência do Teorema 8, tem-se o Corolário 5.

Corolário 5. Se p é um número primo então $p \mid (a^p - a)$, $\forall a \in \mathbb{Z}$.

O Corolário 5 pode ser reescrito e representado na forma de congruência, conforme o apresentado no Corolário 6.

Corolário 6. Sejam p primo e a um número inteiro qualquer, então $a^p \equiv a \ mod\ p$.

Demonstração. Como a é um número inteiro qualquer, tem-se duas possibilidades para verificar: (i) se $p \nmid a$ e (ii) se $p \mid a$.

(i) Se $p \nmid a$, então pelo Teorema 8, tem-se que: $a^{p-1} \equiv 1 \ mod\ p \overset{\cdot a}{\Rightarrow} \ a^p \equiv a \ mod\ p$.

(ii) Se $p \mid a$, então $a \equiv 0 \ mod\ p$, consequentemente, $a^p \equiv 0 \ mod\ p \Rightarrow a^p \equiv a \ mod\ p$.

$\therefore a^p \equiv a \ mod\ p$.

■

Agora, com os conceitos vistos até este momento, é possível adentrar no tópico criptografia. Na criptografia RSA os conceitos tornam-se ferramentas essenciais para uma melhor compreensão das etapas de codificação e decodificação, a partir do uso de chaves e procedimentos que colaboram para o processo de segurança da informação secreta.

2.7 Fundamentos Matemáticos - ECC

Para ter-se uma pequena compreensão sobre o tema Criptografia de Curvas Elípticas - ECC, pois o intuito é apenas mostrar outro método além do RSA, serão abordados os tópicos: grupos abelianos e corpos finitos ou de Galois.

2.7.1 Grupos abelianos

Os grupos são geralmente utilizados para organizar objetos e seres que possuem características em comum, como comportamentos e padrões observáveis. Por exemplo, o grupo formado por números primos tem como característica em comum o fato de serem divisíveis apenas por eles mesmos e por um.

Para o objetivo deste projeto, o Grupo será abordado com um enfoque mais matemático, pensando na sua constituição a partir de um conjunto e de uma operação fechada definida neste mesmo conjunto indicado. Um exemplo de um operação fechada é a adição dos números naturais mostrada neste trabalho.

Coutinho (2023, p. 147) afirma que, "Um conjunto G no qual está definida uma operação $\bigstar$ é um grupo se a operação satisfaz as propriedades: fechamento, associatividade, elemento neutro e elemento inverso."Além disso, um grupo que também satisfaz a comutatividade é chamado de *grupo abeliano*.

Definição 11. Um conjunto G no qual está definida uma operação binária, denotada por $\bigstar$, é um grupo abeliano se a operação satisfaz as seguintes propriedades:

(i) Fechamento: se $a, b \in G \Rightarrow a \bigstar b \in G$.

(ii) Associatividade: dados $a, b, c \in G$ tem-se que $a \bigstar (b \bigstar c) = (a \bigstar b) \bigstar c$.

(iii) Comutativa: $\forall a, b \in G$, $a \bigstar b = b \bigstar a$.

(iv) Elemento neutro: $\exists e \in G$, tal que $\forall a \in G$, $a \bigstar e = e \bigstar a = a$.

(v) Elemento inverso: dado um elemento $a \in G$ qualquer, $\exists a' \in G$ (o inverso de a), tal que $a \bigstar a' = a' \bigstar a = e$.

Vale ressaltar que "quando a operação de um grupo é a adição, trata-se de um *grupo aditivo*, e quando for a multiplicação, o grupo é *multiplicativo*"(COUTINHO, 2023, p. 148). Por exemplo, "o conjunto $\mathbb{Z}_n$ dos inteiros positivos *mod n* com a operação de soma *mod n* é um grupo aditivo (OKIDA, 2011, p. 77).

Em relação ao número de elementos de um grupo, pode-se ter elementos finitos e infinitos. No caso de G ser finito, o valor que representa a quantidade de elementos será denominada *ordem do grupo G*.

Na criptografia de curvas elípticas também utiliza-se grupos cíclicos, "onde são definidos uma ordem n, que é o número de elementos do grupo, e um elemento gerador"(PEREIRA,

2011, p. 24). Assim, "sendo G um grupo cíclico, todos os elementos de G são múltiplos de um elemento particular $g \in G$."(OLIVEIRA, 2010, p. 26). Desta forma, o elemento g é um denominado um gerador do grupo G.

Por exemplo, "um grupo aditivo G é cíclico se $\exists P \in G$, tal que $\forall Q \in G$ pode ser escrito como o produto P com um escalar inteiro λ, isto é, $Q = \lambda P$. Além disso, um elemento P com essa propriedade é chamado de gerador de G."(ARAUJO, 2013, p. 55)

2.7.2 Corpos finitos

Nas curvas elípticas, "os grupos finitos mais usados são os inteiros módulo um número primo, ou um grupo de Galois cujo tamanho é potência de 2 (OKIDA, 2011, p. 27). Essas estruturas algébricas contribuem para detectar e corrigir erros em dados transmitidos a partir de "códigos corretores de erros."(POSSIGNOLO, 2012, p. 23)

Definição 12. Um corpo é um conjunto K, munido de duas operações, adição e multiplicação, que satisfazem a certas propriedades:

(i) $(K, +)$ é um grupo abeliano aditivo com identidade (aditiva) 0;

(ii) $(K \setminus \{0\}, \cdot)$ é um grupo abeliano multiplicativo com identidade (multiplicativa) 1;

(iii) Distributividade: $a \cdot (b + c) = a \cdot b + a \cdot c$, $\forall a, b, c \in K$.

Note que, se o conjunto K é finito, então o corpo é finito. Além disso, o número de elementos do corpo indica a ordem do corpo.

Agora, é possível estudar sobre o tema Criptografia. Sendo assim, no próximo capítulo, serão vistos: O que é criptografia? O que são chaves? Como funcionam os métodos RSA e ECC? Também será mostrado um exemplo com o passo a passo do método RSA, desde a pré-codificação até a decodificação.

Capítulo 3

Criptografia

A criptografia pode ser definida, neste momento, como um processo de transformação de uma informação legível (mensagem original), a partir do uso de uma chave secreta, em uma informação ilegível (criptograma). Em relação aos tipos de operações de transformação utilizadas nesse processo, destacam-se a *substituição* e a *transposição*, conforme ilustrado na Figura 1.8. Já a forma de processamento da mensagem, pode ser em formato de blocos ou por fluxo (stream).

A chave é um elemento muito importante que permite variar o processo de cifragem ou de codificação. Essa distinção nas chaves permite diferentes tipos de criptografia, como a simétrica (também conhecida como convencional ou de chave privada) e a assimétrica (comumente chamada de chave pública).

A diferença entre as chaves é que na simétrica, tanto o remetente quanto o destinatário utilizam uma mesma chave para criptografar e descriptografar, sendo os únicos a conhecerem, e devido a isso chama-se chave privada. Já na assimétrica, o remetente e destinatário utilizam chaves distintas, sendo uma pública e outra privada.

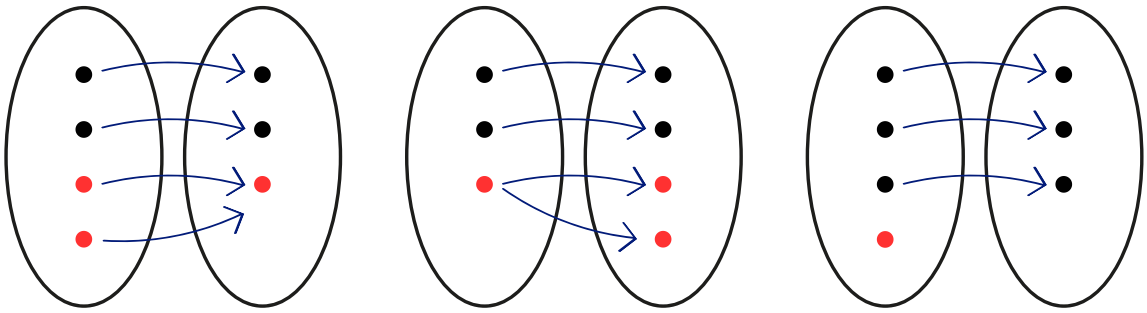
Segundo Oliveira (2010, p. 23),"Em 1976, Whitfield Diffie e Martin Hellman introduziram o conceito de criptografia assimétrica ou de chave pública". Isso abriu caminho para "um mecanismo mais sofisticado publicado em 1978 por Rivest, Shamir e Adleman, conhecido como RSA."(ARAUJO, 2013, p. 4) Além destes, existe o algoritmo de ElGamal, baseado em curvas elípticas e emparelhamentos bilineares.

A criptografia possui muitas aplicações, sendo uma delas nos serviços de segurança, com o intuito de se manter a confidencialidade, integridade, autenticidade e irretratabilidade. Para as empresas é uma ferramenta essencial para proteção de estratégias, segredos, resultados, investimentos, vendas, além da autoproteção de seus funcionários e clientes.

Embora muitas pesquisas apontem que os sistemas criptográficos atuais possam ser quebrados por computadores quânticos, outras pesquisas voltadas para o movimento pós-quântico surgem como uma resposta a essa ameaça, buscando desenvolver algoritmos e protocolos que resistam aos ataques.

Para entender o funcionamento de um bom sistema criptográfico, veja a Figura 3.1.

Figura 3.1: Diagrama com situações criptográficas hipotéticas

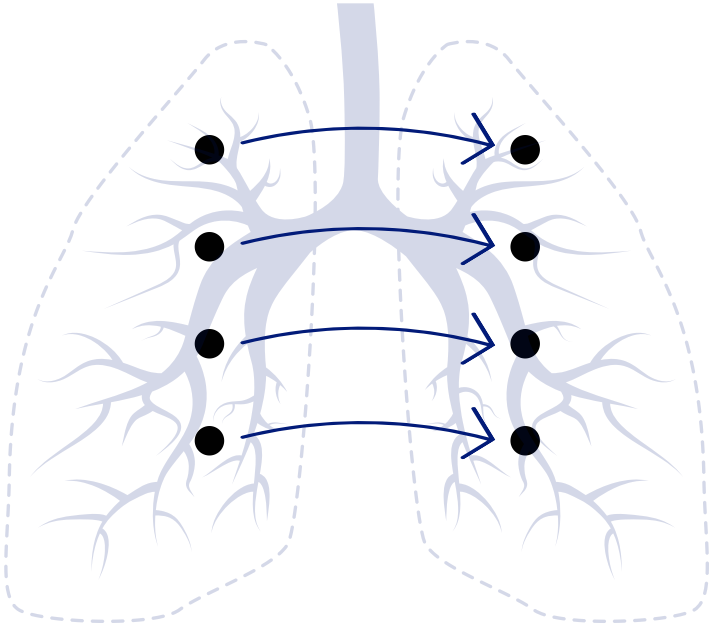


Fonte: Elaborado pelo autor, 2024.

Observe que na primeira situação da Figura 3.1, as mensagens de entrada (em vermelho) geram a mesma mensagem de saída. No segundo diagrama, a entrada gera duas saídas distintas. Já no último diagrama, a mensagem de entrada não possui saída. Essas situações representam falhas em um sistema criptográfico, como ambiguidade, dúvida ou erro de conversão.

Assim como a respiração nos permite viver ao transformar o ar que inspiramos em oxigênio vital para nossas células, um sistema criptográfico impecável depende da função bijetora para funcionar perfeitamente, possibilitando que cada mensagem de entrada tenha uma e apenas uma mensagem de saída correspondente. Essa função, representada na Figura 3.2, atua como os pulmões da criptografia, garantindo a integridade e a reversibilidade do processo de ciframento e deciframento.

Figura 3.2: Diagrama criptográfico ideal



Fonte: Elaborado pelo autor, 2024.

3.1 Criptografia RSA

A criptografia ao passar do tempo aperfeiçoou-se de forma bastante expressiva, e um dos sistemas criptográficos atuais com relevância no mercado é o RSA, bastante utilizado em transações bancárias e comerciais. A sigla RSA, como mencionado anteriormente, corresponde às iniciais dos sobrenomes de seus inventores: Rivest, Shamir e Adleman. Além disso, o método RSA "é baseado na dificuldade computacional de fatorar um número inteiro em primos"(NAKAMURA, 2011, p. 14)

Para mais, os tópicos abordados até aqui contribuem para o entendimento de sua funcionalidade e aplicação, possibilitando o uso de números primos como chave do RSA, escolhendo-os da melhor forma possível, para não comprometer o nível de segurança do sistema criptográfico.

Em relação a sua aplicação em sala de aula, a criptografia RSA será utilizada de forma adaptada, retomando alguns conceitos já vistos em anos anteriores, como: números primos, múltiplos, divisibilidade, decomposição em fatores primos e potenciação. Em seguida, uma analogia do funcionamento de um sistema criptográfico ideal (Figura 3.2), relacionando-o com o conceito de função polinomial do 1° grau no contexto de conjuntos de entrada e saída de mensagens e de dados. Além disso, serão mostradas aplicações do método RSA no cotidiano dos estudantes, tais como: Instagram, TikTok, YouTube, WhatstApp e e-mail.

Agora, veja todo o processo de aplicação do método RSA. Inicia-se pela etapa de pré-codificação, em que relaciona-se o alfabeto, símbolos e algarismos a uma tabela de conversão, seguida da codificação, em que se converte a mensagem desejada de acordo com a tabela, e, finalmente, a etapa de decodificação, que reverte o processo para chegar na mensagem que foi enviada. Também será ilustrado um exemplo que abordará todas as etapas do método para a mensagem: UFSCar 2024.

3.1.1 Pré-codificação

Nesta etapa, realiza-se o processo de conversão da mensagem em uma sequência de números, denominado fase de pré-codificação (Tabela 3.1). Assim, para converter as letras do alfabeto em números utiliza-se uma tabela de conversão, da mesma forma como os algarismos de 0 a 9. Em relação aos espaços, serão substituídos pelo número 41.

Tabela 3.1: Pré-codificação do alfabeto

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
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
-	0	1	2	3	4	5	6	7	8	9															
41	42	43	44	45	46	47	48	49	50	51															

Fonte: Elaborado pelo autor, 2024.

Iniciar a tabela de conversão acima em 1 gera ambiguidade no processo de pré-codificação, pois diferentes combinações de letras podem resultar no mesmo número. Por exemplo, se B fosse convertido por 2 e C por 3, BC e W seriam convertidos para 23, dificultando a interpretação da mensagem codificada. Para solucionar esse problema, sugere-se iniciar a tabela de conversão em um número maior ou igual a 10 (para que toda conversão possua dois dígitos e elimine a ambiguidade), ou utilizar letras ou símbolos adicionais.

Agora, deve-se escolher dois números primos positivos ímpares distintos: suponha que foram escolhidos p e q, eles serão chamados de *parâmetros RSA*. Em seguida, seja $n = p \cdot q$, que será denominado *módulo RSA*. Segundo Carneiro (2017, p. 80), "a última etapa do processo de pré-codificação consiste em separar numa sequência de números ou blocos o longo número produzido. E denominaremos cada bloco de um certo b e devem ser números menores que n".

CARNEIRO ressalta também que é importante evitar duas situações:

1. Nenhum bloco deve começar com o número zero, pois gera problema na decodificação.

2. Os blocos não devem corresponder a nenhuma unidade linguística (palavra, letra, etc.). Assim, a decodificação por contagem de frequência fica inviável.

3.1.2 Codificando

Após a pré-codificação tem-se a codificação. Para codificar utiliza-se o produto dos primos vistos anteriormente: $n = p \cdot q$ e de um inteiro positivo e que seja inversível módulo $\phi(n)$, ou seja, o $mdc\ (e, \phi(n)) = 1$. Assim, a *chave de codificação* ou *chave pública* é o par (n, e), com $f = \phi(n) = (p-1) \cdot (q-1)$.

Como caracteriza Coutinho (2023, p. 188), "$C(b)$ é o resultado da codificação do bloco $0 \leq b \leq n-1$". Desta maneira, $C(b) =$ *resto da divisão de* b^e *por* n. Esse cálculo é realizado com base na aritmética modular, em que $C(b)$ corresponde ao resíduo de b^e módulo n. Assim, podemos reescrever a expressão de codificação: $C(b) \equiv b^e\ (mod\ n)$.

3.1.3 Decodificando

A etapa de decodificação da mensagem é realizada utilizando o n e o inverso de e módulo $f = \phi(n)$, que será denotado por um inteiro positivo d. Desta forma, o par (n, d) será chamado de *chave privada* ou *chave de decodificação*.

Para calcular os inversos em aritmética modular pode-se usar o algoritmo euclidiano estendido, mas se o inverso obtido é negativo, escolhe-se para d seu resíduo módulo f. Por outro lado, se o par (n, d) é a chave secreta e o par (n, e) a chave pública, então a decodificação de $a = C(b)$ é definida por: $D(a) \equiv a^d\ (mod\ n)$, em que a é um bloco de mensagem codificada e $D(a)$ o resultado da decodificação.

3.1.4 Codificando e Decodificando - UFSCar 2024

Para ilustrar as etapas descritas nos tópicos anteriores, será codificado a mensagem: UFSCar 2024. Inicialmente, a fase de pré-codificação seguindo a Tabela 3.1 de conversão, obtendo-se a sequência indicada na Tabela 3.2.

Tabela 3.2: Pré-codificação da mensagem: UFSCar 2024

U	F	S	C	A	R	-	2	0	2	4
35	20	33	17	15	32	41	44	42	44	46

Fonte: Elaborado pelo autor, 2024.

A conversão da mensagem UFSCar 2024 resulta em **35203317153241444244446**. Agora, escolhe-se dois números primos distintos, por exemplo: $p = 17$ e $q = 11$, então tem-se $n = p \cdot q = 17 \cdot 11 = 187$ e $\phi(n) = (p-1) \cdot (q-1) = 16 \cdot 10 = 160$. Em seguida, precisa-se escolher um número inteiro e tal que $(e, \phi(n)) = 1$, por exemplo $e = 7$.

O próximo passo é separar a mensagem em blocos, e estes blocos podem ter tamanhos distintos de algarismos, mas cada um deles precisa respeitar uma condição, que é ser menor que a chave de codificação $n = 187$. Sendo assim, tem-se: $35 - 20 - 33 - 171 - 5 - 32 - 4 - 144 - 42 - 44 - 46$.

Posteriormente, codifica-se cada bloco com base na chave pública criada $(n, e) = (187, 7)$, e utilizando a expressão de codificação: $C(b) \equiv b^e \ (mod\ n)$.

(i) Bloco 35: $C(35) \equiv 35^7 \ (mod\ 187) \equiv 18 \ (mod\ 187) \Rightarrow C(35) = 18$.

(ii) Bloco 20: $C(20) \equiv 20^7 \ (mod\ 187) \equiv 147 \ (mod\ 187) \Rightarrow C(20) = 147$.

(iii) Bloco 33: $C(33) \equiv 33^7 \ (mod\ 187) \equiv 33 \ (mod\ 187) \Rightarrow C(33) = 33$.

(iv) Bloco 171: $C(171) \equiv 171^7 \ (mod\ 187) \equiv 52 \ (mod\ 187) \Rightarrow C(171) = 52$.

(v) Bloco 5: $C(5) \equiv 5^7 \ (mod\ 187) \equiv 146 \ (mod\ 187) \Rightarrow C(5) = 146$.

(vi) Bloco 32: $C(32) \equiv 32^7 \ (mod\ 187) \equiv 76 \ (mod\ 187) \Rightarrow C(32) = 76$.

(vii) Bloco 4: $C(4) \equiv 4^7 \ (mod\ 187) \equiv 115 \ (mod\ 187) \Rightarrow C(4) = 115$.

(viii) Bloco 144: $C(144) \equiv 144^7 \ (mod\ 187) \equiv 100 \ (mod\ 187) \Rightarrow C(144) = 100$.

(ix) Bloco 42: $C(42) \equiv 42^7 \ (mod\ 187) \equiv 15 \ (mod\ 187) \Rightarrow C(42) = 15$.

(x) Bloco 44: $C(44) \equiv 44^7 \ (mod\ 187) \equiv 22 \ (mod\ 187) \Rightarrow C(44) = 22$.

(xi) Bloco 46: $C(46) \equiv 46^7 \ (mod\ 187) \equiv 7 \ (mod\ 187) \Rightarrow C(46) = 7$.

Logo, a mensagem codificada é: **181473352146761151001522 7**.

Para executar o processo de decodificação, precisa-se determinar o valor de d tal que $7d \equiv 1 \ (mod\ 160) \Leftrightarrow 7d = 160 \cdot k + 1$, com $d < 160$ e $k \in \mathbb{Z}_+$. Desse modo, como $7d = 160 \cdot k + 1 \Rightarrow 7d + 160(-k) = 1$.

Sabe-se que $\phi(n) = 160$ e $e = 7$, então ainda falta determinar d e k, que podem ser encontrados a partir das divisões sucessivas:

(i) $160 = 7 \cdot 22 + 6 \Rightarrow 6 = 160 - 7 \cdot 22$;

(ii) $7 = 6 \cdot 1 + 1 \Rightarrow 1 = 7 - 6 \cdot 1$;

(iii) $6 = 1 \cdot 6 + 0$.

Como em (ii) tem-se $1 = 7 - 6 \cdot 1 \overset{\text{(i)}}{\Rightarrow} 1 = 7 - (160 - 7 \cdot 22) \cdot 1 \overset{\text{dist.}}{\Rightarrow} 7 \cdot 1 + 7 \cdot 22 - 160 \cdot 1 = 7(23) + 160(-1)$. Logo, $d = 23$ e $k = 1$.

Sabe-se que o par (n, d) é a chave privada, então com base no valor encontrado para d, tem-se: $(n, d) = (187, 23)$. Em seguida, usa-se a expressão $D(a) \equiv a^d \ (mod\ n)$ em cada bloco codificado, para obter-se o resultado da decodificação.

(i) Bloco 18: $D(18) \equiv 18^{23} \ (mod\ 187) \equiv 35 \ (mod\ 187) \Rightarrow D(18) = 35$.

(ii) Bloco 147: $D(147) \equiv 147^{23} \ (mod\ 187) \equiv 20 \ (mod\ 187) \Rightarrow D(147) = 20$.

(iii) Bloco 33: $D(33) \equiv 33^{23} \ (mod\ 187) \equiv 33 \ (mod\ 187) \Rightarrow D(33) = 33$.

(iv) Bloco 52: $D(52) \equiv 52^{23} \ (mod\ 187) \equiv 171 \ (mod\ 187) \Rightarrow D(52) = 171$.

(v) Bloco 146: $D(146) \equiv 146^{23} \ (mod\ 187) \equiv 5 \ (mod\ 187) \Rightarrow D(146) = 5$.

(vi) Bloco 76: $D(76) \equiv 76^{23} \ (mod\ 187) \equiv 32 \ (mod\ 187) \Rightarrow D(76) = 32$.

(vii) Bloco 115: $D(115) \equiv 115^{23} \ (mod\ 187) \equiv 4 \ (mod\ 187) \Rightarrow D(115) = 4$.

(viii) Bloco 100: $D(100) \equiv 100^{23} \ (mod\ 187) \equiv 144 \ (mod\ 187) \Rightarrow D(100) = 144$.

(ix) Bloco 15: $D(15) \equiv 15^{23} \ (mod\ 187) \equiv 42 \ (mod\ 187) \Rightarrow D(15) = 42$.

(x) Bloco 22: $D(22) \equiv 22^{23} \ (mod\ 187) \equiv 44 \ (mod\ 187) \Rightarrow D(22) = 44$.

(xi) Bloco 7: $D(7) \equiv 7^{23} \ (mod\ 187) \equiv 46 \ (mod\ 187) \Rightarrow D(7) = 46$.

Observe que o resultado do processo de decodificação coincide com a etapa de pré-codificação: **3520331715324144424446**. Assim, comparando os valores decodificados com a Tabela 3.1, confirma-se que a mensagem original é UFSCar 2024.

Como visto até aqui o RSA utiliza dois primos ímpares positivos distintos, como, por exemplo, o p e q. Também utiliza dois pares de chaves, sendo (n, e) a chave pública e (n, d) a chave privada, em que a primeira codifica e a segunda decodifica. Como (n, e) é

pública, qualquer pessoa pode ter acesso a ela, então "o RSA só será seguro na medida em que for difícil calcular d quando apenas n e e são conhecidos"(COUTINHO, 2023, p. 190). Além disso, por se tratar do uso de chaves diferentes para os processos de codificação e decodificação, denomina-se este método de criptografia assimétrica.

O RSA "baseia-se na facilidade de gerar números primos grandes e na dificuldade prática de fatorar o produto de dois desses números"(HEFEZ, 2022, p. 218). Essa segurança, segundo Carneiro (2017, p. 91), está intimamente ligada "à inexistência de ferramentas eficientes para fatoração rápida". Além disso, o sistema fundamenta-se em propriedades e teoremas vistos em disciplinas como Teoria dos Números (Graduação) e Aritmética (Pós-graduação), em tópicos como Divisão Euclidiana, Fatoração de Fermat, Aritmética Modular e Criptografia.

O método RSA é uma das ferramentas mais utilizadas atualmente quando se fala em criptografia assimétrica. No entanto, outro método que vem ganhando destaque é o ECC (Criptografia de Curvas Elípticas). Embora a compreensão do ECC envolvam temas matemáticos complexos, em sala de aula serão apresentadas as curvas elípticas usando o Geogebra. Isso ajudará aos alunos a perceber que é necessário construir uma bagagem matemática ao longo dos anos para realizar aplicações mais complexas em áreas como a da segurança da informação.

Por outro lado, é possível apresentar e desenvolver um tema complexo de forma mais simples, de modo a conquistar o interesse e o engajamento dos estudantes. Dessa forma, eles serão estimulados a encarar os desafios de maneira diferente, começando com o que já sabem e buscando aprender o que ainda precisam.

3.2 Criptografia de Curvas Elípticas - ECC

A criptografia de curvas elípticas (Ou Elliptic Curve Cryptography – ECC) é um método que utiliza a criptografia de chave pública fundamentada em curvas elípticas sobre corpos finitos. Para entender às curvas elípticas, precisa-se, inicialmente, compreender como elas se originam, que é a partir de equações cúbicas. De acordo com Okida (2011, p. 15), "as curvas elípticas sobre o corpo dos números reais vêm a ser dadas por equações na forma Weierstraß (também conhecido como Karl Weierstrass): $y^2 = x^3 - x$ e por $y^2 = x^3 - x + 1$".

Segundo Oliveira (2010, p. 24), "uma curva elíptica pode ser definida sobre qualquer corpo, mas para aplicações criptográficas elas costumam ser definidas sobre corpos finitos (corpos binários e corpos primos)". Assim, uma curva elíptica E sobre um corpo algébrico fechado K, abrange todos os elementos (x, y), chamados de pontos na curva, que satisfazem a equação de Weierstrass.

Definição 13. Uma curva elíptica E sobre um corpo K, denotada E/K, é definida pela equação:

$$E(K) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.1}$$

em que os coeficientes $a_1, a_2, a_3, a_4, a_6 \in K$ e $\Delta \neq 0$, sendo Δ o discriminante de E. Além disso, a curva $E(K)$ possui ainda um ponto extra, chamado de ponto no infinito, que será representado por O.

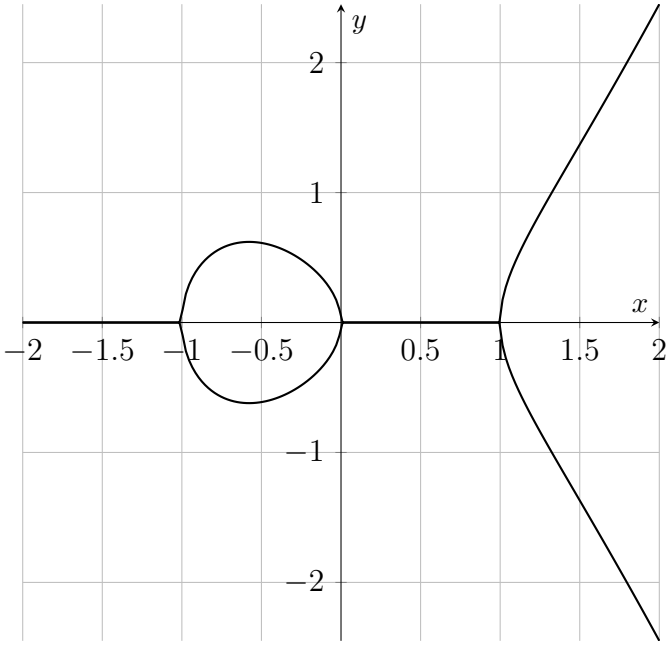
Como afirma Pereira (2011, p. 29), "o discriminante Δ serve para indicar se a equação da curva $E(K)$ corresponde ou não a uma equação cúbica singular. Ser não singular significa que a equação cúbica $y^2 = f(x)$ não possui raízes repetidas". Desse modo, uma curva elíptica com $\Delta = 0$ é chamada de singular, e com $\Delta \neq 0$ é chamada de não singular.

O Δ é definido da seguinte forma:
$$\begin{cases} \Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 = a_1^2 + 4a_2 \\ d_4 = 2a_4 + a_1a_3 \\ d_6 = a_3^2 + 4a_6 \\ d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^3. \end{cases}$$

Nas Figuras 3.3 e 3.4 é possível observar curvas elípticas sobre o corpo K dos números reais. A primeira é uma curva elíptica não-singular: $y^2 = x^3 - x$, que possui três raízes reais distintas. Já a segunda, é uma curva singular: $y^2 = x^3 + x$, que apresenta uma única raiz real.

Para encontrar as raízes precisa-se determinar as intersecções com o eixo x, isto é, valores de x para os quais o $y = 0$. Assim, na curva não-singular, tem-se: $0^2 = x^3 - x \Rightarrow x(x^2 - 1) = 0 \Rightarrow x(x + 1)(x - 1) = 0$. Logo as raízes reais são: $x = 0$, $x = 1$ ou $x = -1$. Também é possível identificar as raízes observando as intersecções com o eixo x nos gráficos apresentados logo adiante.

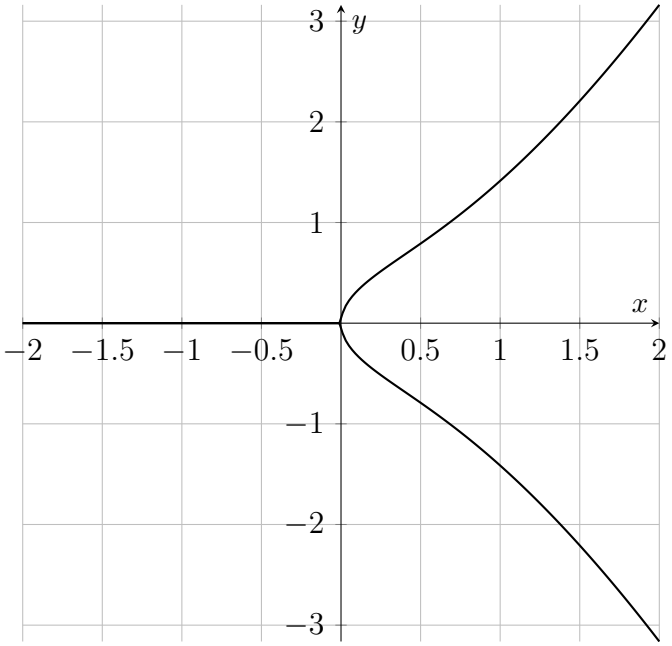
Figura 3.3: Curva elíptica não-singular: $y^2 = x^3 - x$



Fonte: elaborado pelo autor.

Note que a curva elíptica singular ($y^2 = x^3 + x$) possui mais de uma raiz, pois para $y = 0$, tem-se: $0^2 = x^3 + x \Rightarrow x(x^2 + 1) = 0 \Rightarrow x = 0$, $x = -\sqrt{-1}$ e $x = \sqrt{-1}$. No entanto, nos reais, a única raiz válida é $x = 0$, porque não será abordado os números complexos. Já em relação a intersecção com o eixo y, basta tomar $x = 0$. Assim, tanto na figura acima quanto na figura abaixo, a intersecção acontece quando o $y = 0$.

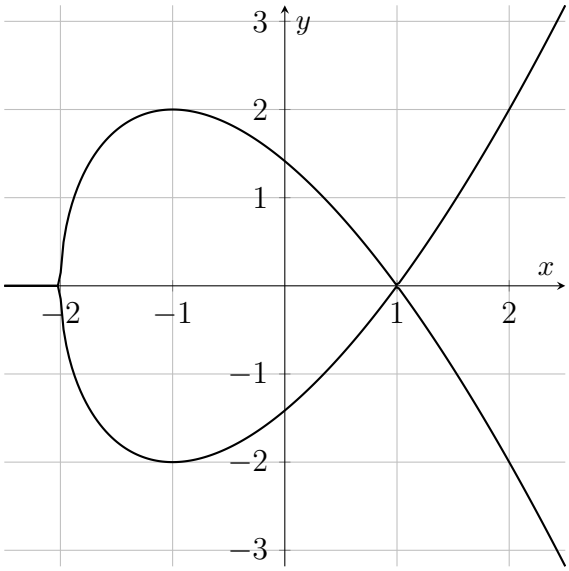
Figura 3.4: Curva elíptica singular: $y^2 = x^3 + x$



Fonte: elaborado pelo autor.

Por exemplo, na curva $y^2 = x^3 - 3x + 2$, tem-se como intersecções com o eixo x: $(-2, 0)$ e $(1, 0)$. Agora, no eixo y a intersecção ocorre em $y = \pm\sqrt{2}$, conforme a Figura 3.5.

Figura 3.5: Curva elíptica: $y^2 = x^3 - 3x + 2$



Fonte: elaborado pelo autor.

De acordo com Nakamura (2011, p. 10), "em uma curva elíptica E/K com $char(K) = p$ *prima* $p \neq 2$, $p \neq 3$ e sendo p grande é chamada *curva prima*". Por outro lado, a Equação 3.1, quando considera-se as curvas primas, sofre uma modificação para a forma:

$$E(K) : y^2 = x^3 + ax + b, \tag{3.2}$$

com $a, b \in K$ e o discriminante $\Delta = 4a^3 + 27b^2 \neq 0$.

Sob outra perspectiva, como $y^2 = (-y)^2$ é possível verificar que o par (x, y) atende a equação 3.2 se, e somente se, $(x, -y)$ também a satisfaz. Consequentemente, o gráfico de uma curva elíptica é sempre simétrico em relação ao eixo x.

Além disso, para encontrar o domínio da equação 3.2, conjunto de valores de x para os quais a equação dada tem solução, realiza-se a análise do sinal de $x^3 + ax + b$. Perceba que $y^2 \geq 0$, então $\exists y$ tal que (x, y) satisfaz a equação 3.2 se, e somente se, $x^3 + ax + b \geq 0$.

O foco deste trabalho não é se aprofundar no tema ECC. Por isso, ele foi mostrado de forma superficial, mas é um método que vem ganhando bastante espaço e sendo utilizado em protocolos de assinatura digital e distribuição segura de chave. De acordo com Arruda (2014, p. 27), "requerem menos recursos computacionais do que o RSA, e permitem a implementação mais eficiente de segurança nos serviços disponíveis em dispositivos sem fio, como e-mail seguro, navegação web e rede privada (VPN)."

Por esse motivo, a necessidade de citá-lo e abordá-lo neste capítulo após o método RSA. Enfim, como já foram vistos diversos tópicos que contribuem para o entendimento dos métodos RSA e ECC, chega-se no momento de relacioná-los e aplicá-los em sala de aula. Sendo assim, no próximo capítulo serão vistos formas de aplicar a Criptografia no Ensino da Matemática em turmas do 9° ano do Ensino Fundamental a partir de jogos, quiz, desafios, história, matemática e diversão.

Capítulo 4

Criptografia no Ensino da Matemática

No panorama educacional contemporâneo, combater as dificuldades de aprendizagem se ergue como um desafio crucial, especialmente para o Professor de Matemática, figura central na busca por melhores resultados em avaliações internas e externas. Ciente dessa realidade e impelido pela responsabilidade docente, será apresentado uma proposta para o ensino de matemática explorando o tópico Criptografia em turmas de 8° e 9º anos do Ensino Fundamental com o intuito de despertar o interesse e o engajamento dos alunos, impulsionando-os na jornada de aprendizagem.

Segundo Silva, Lima e Andriola (2016, p. 90):

> Os futuros professores devem ser preparados para enfrentar os desafios atuais de uma sociedade em constante mudança. Para isso, é fundamental que ocorram mudanças significativas na elaboração e execução de cursos que abordem especificamente a formação de professores.

Essa visão encontra ressonância nas palavras de Moran (2015, p. 29), que destaca "a importância de as instituições educacionais estarem atentas às mudanças". O autor apresenta duas alternativas: "um caminho mais suave, com alterações progressivas, e outro mais amplo, com mudanças profundas".

Nesse cenário de transformações, surge a ideia de que os discentes sejam protagonistas de seu próprio conhecimento, com os professores atuando como mediadores nesse processo. Logo, é algo que vai além de técnicas, tornando-se uma proposta de mudança na relação professor-aluno e aluno-professor. O professor assume o papel de orientador, mediador e organizador da interação entre os estudantes, enquanto o aluno se torna o protagonista de sua aprendizagem, assumindo a responsabilidade principal pelo processo de aprendizado.

Como descrito por D'ambrosio (2012, p. 63), "a educação é uma estratégia da sociedade para facilitar que cada indivíduo atinja o seu potencial e para estimular cada indivíduo a colaborar com outros em ações comuns na busca do bem comum". Sem dúvida, a educação contribui bastante para que o estudante alcance o seu potencial, mas a escola precisa atuar em conjunto com a família e comunidade para atingir este objetivo, pois existe

uma engrenagem que gira com vários agentes que estende-se para algo além da relação aluno-professor e professor-aluno.

Por isso, esta proposta consiste na implementação de estratégias pedagógicas dinâmicas e envolventes, que transcendem o modelo tradicional de ensino e constroem pontes entre a teoria e a prática, tornando a matemática mais acessível e significativa para os alunos. "Um projeto de personalização que realmente atenda aos estudantes requer que eles, juntos com o professor, possam delinear seu processo de aprendizagem, selecionando recursos que mais se aproximam de sua melhor maneira de aprender" (BACICH; NETO; TREVISANI, p. 51).

Nesse sentido, para alcançar os objetivos propostos, foi idealizada uma atividade sobre Criptografia em formato de rotação por estações de aprendizagem, em que os grupos de estudantes passam pelas estações de aprendizagem e aprendem sobre Criptografia em diferentes abordagens. Através dessa experiência lúdica e envolvente, os participantes terão a oportunidade de colocar em prática seus conhecimentos matemáticos e criptográficos, desvendando enigmas e desafios que estimularão o desenvolvimento de diversas habilidades essenciais.

De acordo com Enkvist (2021, p. 54):

> O professor deve lembrar que, para os alunos, certas aulas acontecem apenas uma vez na vida e o professor é responsável por tornar aquela aula memorável. Os alunos são sempre diferentes e os momentos também o são. Portanto, cada aula é algo novo e, no mínimo, deve haver uma adaptação de algo feito anteriormente, em outras ocasiões.

A rotação por estações de aprendizagem é uma boa estratégia para trabalhar a Criptografia, em que cada grupo passa por uma estação de aprendizagem, resolve o desafio, e segue para próxima estação, sem a necessidade de precisar seguir a mesma ordem de percurso, apenas tendo uma única condição, que é a de passar por todas as estações criadas, e, assim, utilizar as informações adquiridas para cumprir o objetivo final: aprender sobre Criptografia.

Nesta atividade em particular, serão utilizados estações sobre os seguintes tópicos:

(i) Cifra com algarismos: os estudantes terão que decodificar seis mensagens codificadas;

(ii) História da Criptografia: descobrir entre as mensagens cifradas as respostas das perguntas indicadas na estação 2, como que tipo de método utilizaram para decifrar as mensagens da rainha escocesa Mary Stuart? Resposta: criptoanálise;

(iii) Cifra com letras: decifrar uma mensagem criptografada a partir da Cifra de César, e identificar a sigla do Estado presente na mensagem original.

(iv) Cifrar a mensagem: A MATEMÁTICA É LINDA. Após isso, realizar a soma total dos valores cifrados obtidos para substituir na função polinomial do 1º grau sugerida.

Além das estações de aprendizagem, outras atividades idealizadas foram: o jogo do labirinto na plataforma *Wordwall* e Quiz na plataforma *Kahoot*. Nestas atividades, as questões são relacionadas ao desenrolar da história da Criptografia, desde a Antiguidade até a Era digital. Também será tratado a diferença entre cifras e códigos, e das criptografias simétricas e assimétricas.

4.1 Jogos como estratégia de ensino

Segundo Martinelli e Martinelli (2016, p. 114): "Houve um tempo em que não se admitia o jogo dentro da sala de aula, pois esse recurso era visto apenas como diversão". No entanto, nos dias de hoje, é um aliado imprescindível, contribuindo para uma avaliação mais divertida, e proporcionando o momento de aprender brincando. Assim, os estudantes se sentem mais a vontade, e participam mais, principalmente em atividades que envolvem a ludicidade aliada a habilidades já adquiridas.

Evidentemente, restringir os jogos apenas para sistematização de uma determinada habilidade não seja a proposta ideal. No entanto, é uma forma de proporcionar um olhar diferenciado para os estudantes, em um momento que oportuniza: observar, mediar e desenvolver algo que tenha passado despercebido. Essa visão vai de encontro com o que afirmam Wiggins e McTIGHE (2019, p. 50), "ter alunos atentos que não entendem nos mostra que o que pensávamos que estava claro na realidade não estava."

Para Zabala (2010, p. 97),

> o ensino não deve se limitar ao que o aluno já sabe, mas que a partir deste conhecimento tem que conduzi-lo à aprendizagem de novos conhecimentos, ao domínio de novas habilidades e à melhora de comportamentos já existentes, pondo-os em situações que o obriguem a realizar um esforço de compreensão e trabalho.

Nesse sentindo, conhecer a turma, os discentes e os conhecimentos prévios que possuem, é uma boa alternativa para um planejamento pedagógico efetivo e assertivo, visto que cada sala possui sua particularidade, e cada estudante é diferente um do outro. Além disso, "na perspectiva do aluno, é a contribuição do professor que dá corpo e presença ao conhecimento."(ENKVIST, 2021, p. 62)

É importante ressaltar que uma estratégia as vezes funciona com a turma X, mas não funciona com a turma Y, pois é necessário levar em consideração diversos aspectos, tanto os fatores facilitadores, que contribuem para uma atividade bem aplicada, quanto os fatores inibidores, que podem dificultar o desenvolvimento de uma habilidade ou a construção de um conhecimento. Como apontam Wiggins e McTIGHE (2019, p. 38), "compreender é ter feito da maneira correta, o que frequentemente se reflete na capacidade de explicar por que uma habilidade, abordagem ou corpo de conhecimento é ou não é apropriado em uma situação específica."

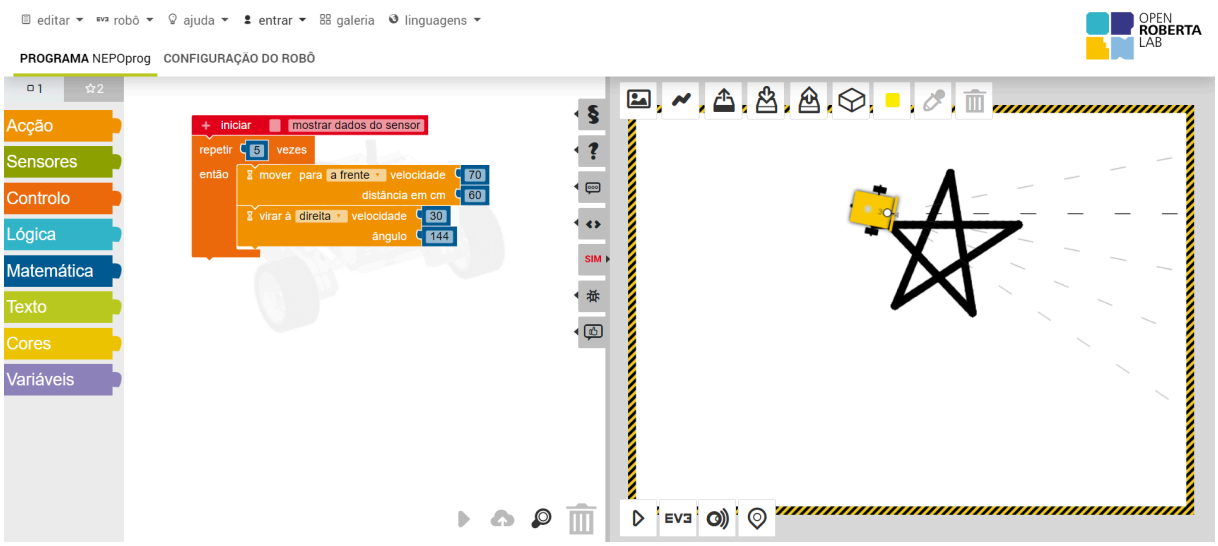
Para aplicação de jogos em sala de aula, nem sempre é necessário fazer uso de tecnologias, pode-se utilizar brincadeiras como: torta na cara com as perguntas impressas, caça ao tesouro com um descritivo de percurso para cada grupo, uno de operações, dominó de frações, pixel art em papel com folha quadriculada etc. Da mesma maneira, se tiver tecnologia a disposição, pode-se aplicar a caça ao tesouro na plataforma padlet (mapas, murais interativos e colaborativos), quiz na plataforma de aprendizagem Kahoot, jogo da forca e labirinto na plataforma Wordwall, entre outras propostas.

Para Bacich, Neto e Trevisani (2015, p. 47-48),

> O uso de tecnologias digitais no contexto escolar propicia diferentes possibilidades para trabalhos educacionais mais significativos para os seus participantes. Entretanto, não devemos esquecer do planejamento de propostas didáticas que busquem *aprender a aprender*, o *aprender a fazer*, o *aprender a ser* e o *aprender a conviver*.

Observe, por exemplo, na Figura 4.1 um desafio de Robótica lançado para as turmas de 8° anos do Ensino Fundamental. A proposta era voltada para o desenvolvimento de uma programação na plataforma Open Roberta Lab com o intuito de fazer o robô percorrer uma pista e desenhar uma estrela pentagonal (pentagrama). Para isso, era necessário saber que o pentagrama é formado por um pentágono regular no centro e cinco triângulos isósceles (cujas bases são os lados do pentágono interno), sendo os ângulos internos do pentágono regular igual a 108° e os ângulos das bases dos triângulos isósceles medindo 72°. Assim, com essas informações e sabendo que a soma dos ângulos internos e externos é igual a 180°, os alunos poderiam determinar os ângulos de giro necessários para que o robô desenhasse cada segmento do pentagrama com precisão.

Figura 4.1: Desafio na Plataforma Open Roberta



Fonte: Elaborado pelo autor, 2024.

Da mesma forma, outra proposta interessante é a utilização de desenhos para trabalhar a matemática. Uma aplicação nesse sentido foi realizada com as turmas de 6º anos do Ensino

Fundamental com os objetos de conhecimento: Frações e Porcentagem. Na atividade, alguns estudantes desenhavam em papel quadriculado em formato pixel art, e outros construíam na plataforma Minecraft Education, conforme a Figura 4.2. Posteriormente, realizavam a contagem da quantidade de quadradinhos (ou de cubinhos no caso do Minecraft), em seguida, montavam as frações das cores utilizadas, e, finalmente, transformavam as frações em porcentagem.

Figura 4.2: Desenho, fração e porcentagem

Fonte: Elaborado pelo autor, 2024.

Isso vai de encontro a afirmação de Borba e Penteado (2019, p. 56), "as inovações educacionais, em sua grande maioria, pressupõem mudança na prática docente, não sendo uma exigência exclusiva que envolvem o uso de tecnologia informática". Nesse contexto, uma reflexão sobre a prática docente contribuirá para o uso de jogos educacionais de forma eficiente, aliado aos recursos disponíveis e a realidade da comunidade em que a Escola está inserida.

Portanto, os jogos como estratégia de ensino, em conjunto com os recursos educacionais disponíveis, podem ser um aliado essencial para construção do conhecimento em sala de aula, com o professor de matemática assumindo o papel de mediador participativo de um processo que possui vários atores ativos e autônomos. Certamente, o aprender fazendo torna tudo mais divertido, contribuindo para que o professor atinja as metas de aprendizagem.

4.1.1 Criptografia no formato de Rotação por Estações de Aprendizagem

A Rotação por estações é um modelo em que "os estudantes são organizados em grupos, cada um dos quais realiza uma tarefa, de acordo com os objetivos do professor para aula em questão. Podem ser realizadas atividades escritas, leituras, entre outras."(BACICH; NETO; TREVISANI, 2015, p. 55) Além disso, um dos grupos precisa estar envolvido com uma proposta que utiliza recursos tecnológicos, sendo bastante importante o uso de recursos visuais, textuais, imagens, entre outras, para enriquecer o ambiente de aprendizagem.

Essa proposta é um modelo presente na metodologia Ensino híbrido, que possibilita aprender de formas diferentes sobre um determinado tema, além de trabalhar de forma coletiva, colaborativa e individual em estações diferentes de aprendizagem. Assim, "cada espaço deve permitir ao aluno utilizar diferentes ferramentas para que busque seu melhor caminho rumo ao completo aprendizado."(SANTOS, 2015, p. 106)

Pensando nessa proposta, foi idealizada uma atividade que realiza a aplicação do tema Criptografia no formato de rotação por estações de aprendizagem, com desafios que contribuem para a desenvolvimento, construção e sistematização dos conhecimentos adquiridos ao longo do processo de ensino e aprendizagem.

A atividade de Rotação por Estações de Aprendizagem sobre Criptografia será realizada da seguinte forma: teremos cinco estações, e cada grupo, composto por 7 ou 8 estudantes, deverá passar por todas elas na ordem que considerar mais conveniente. As estações abordarão diferentes aspectos da criptografia, incluindo sua história, com textos criptografados retirados desta dissertação, mensagens codificadas e cifradas, além do jogo "Perseguição no Labirinto"na plataforma Wordwall. Após a conclusão das atividades em todas as estações, realizou-se um quiz no Kahoot e a aplicação de um formulário no Forms para avaliar o que foi aprendido e coletar feedback sobre o que acharam do projeto.

Para realizar os desafios sugeridos, todos os grupos terão à disposição um documento com roteiro, explicações e espaço para cálculos e respostas, bem como as Tabelas 4.1, 4.2 e 1.1, que servirão de apoio para conseguirem chegar na solução.

Estação 1. *(Decifração da Cifra com algarismos)* Na primeira estação, os estudantes precisam decifrar uma mensagem que utiliza criptografia simétrica, isto é, um sistema que usa a mesma chave para cifrar e decifrar dados. Assim, é preciso usar a Tabela 4.1 para decodificar as mensagens dos desafios propostos.

Desafio 1. 24283625272415142828242714283628142225271436161023171022362324361530292810213613143613241828361036351427 24.

(i) Mensagem decifrada: Os professores sempre ganham no futsal de dois a zero.

Desafio 2. 24361127102818213612242326301828292430361218231224361224251028361324362230231324.

(i) Mensagem decifrada: O Brasil conquistou cinco Copas do mundo.

Desafio 3. 10362810211036131436103021103625242828301836292718232910361436132418283614282930131023291428.

(i) Mensagem decifrada: A sala de aula possui trinta e dois estudantes.

Desafio 4. 10361227182529241627101518103614271036302918211835101310362510271036252724291416142736221423281016142328361224231518131423121810182836142236291422252428361314361630142727103614361428251824231016142 2.

(i) Mensagem decifrada: A criptografia era utilizada para proteger mensagens confidenciais em tempos de guerra e espionagem.

Desafio 5. 24283612242225302910132427142836242514271022362310362118231630101614223611182310271810.

(i) Mensagem decifrada: Os computadores operam na linguagem binária.

Desafio 6. 10361227182529241627101518103628182214292718121036302918211835103630221036302318121036121710311436251027103612271825292416271015102736143613142812271825292416271015102736182315242722101224142 8.

(i) Mensagem decifrada: A criptografia simétrica utiliza uma única chave para criptografar e descriptografar informações.

Tabela 4.1: Estações 1 e 4 - Chave: $y = x + 9$

Alfabeto	Posição	Codificação
A	1	10
B	2	11
C	3	12
D	4	13
E	5	14
F	6	15
G	7	16
H	8	17
I	9	18
J	10	19
K	11	20
L	12	21
M	13	22
N	14	23

Alfabeto	Posição	Codificação
O	15	24
P	16	25
Q	17	26
R	18	27
S	19	28
T	20	29
U	21	30
V	22	31
W	23	32
X	24	33
Y	25	34
Z	26	35
-	27	36

Fonte: Elaborado pelo autor, 2024.

Na segunda estação o desafio será voltado para uma exploração sobre: A história da Criptografia. Os tópicos da Antiguidade a Era Digital serão abordados e discutidos em sala de aula, e na estação ficarão disponíveis apenas alguns textos da parte histórica deste trabalho.

Estação 2. *(Decifração - letras)* Encontre, entre os quatro recortes de textos disponibilizados com base na Cifra de César (os recortes foram retirados do capítulo 1 deste trabalho), as respostas para o Desafio 7. Para decifrar os recortes, utilize a Tabela 1.1.

Recorte 1. D FULSWRJUDILD SRVVXL XPD KLVWRULD ULFD H FRPSOHAD TXH VH HQWUHODFD FRP R GHVHQYROYLPHQWR GD FLYLOLCDFDR KXPDQD. GHVGH RV SULPRUGLRV GD HVFULWD DWI D HUD GD FRPSXWDFDR TXDQWLFD, D EXVFD SRU PHWRGRV VHJXURV GH FRPXQLFDFDR WHP PROGDGR D IRUPD FRPR SURWHJHPRV LQIRUPDFRHV FRQILGHQFLDLV.

Recorte 2. D FLIUD GH VXEVWLWXLFDR PRQRDOIDEHWLFD GH FHVDU, HPERUD VLPSOHV QD VXD FRQFHSFDR, IRL XPD IHUUDPHQWD LQHVWLPDYHO SDUD D FRPXQLFDFDR VHFUHWD HP WHPSRV GH EDLAD DOIDEHWLZAFDR. VXD UHOHYDQFLD UHVLGH QDR DSDQDV QD VXD HIHWLYLGDGH SUDWLFD, PDV WDPEHP QR SDSHO TXH GHVHPSHQKRX FRPR SUHFHUVRU GRV PHWRGRV PRGHUQRV GH FULSWRJUDILD, DEULQGR FDPLQKR SDUA XP PRQGR RQGH D VHJXUDQFD GD LQIRUPDFDR VH WRUQRX FDGD YHC PDLV FUXFLDO.

Recorte 3. D KLVWRULD UHJLVWUD D SULPHLUD YLWLPD IDPRVD SRU FDXVD GD VHJXUDQFD GH VXDV PHQVDJHQV FULSWRJUDIDGDV: PDUB VWXDUW GA HVFRFLD. DV PHQVDJHQV GD UDLQKD HVFRFHVA IRUDP GHFLIPADAV SRU PHLR GR PHWRGR GH FULSWRDQDOLVH, SHUPLWLQGR TXH DV FDUWDV IRVVHP XVDGDV FRPR SURYDV GH FRQVSLUDFDR FRQWUD VXD SULPD, UDLQKD HOLCDEHWK SULPHLUD GA LQJODWHUUD.

Recorte 4. D PDUB VWXDUW DSUHQGHX D FULSWRJUDIDU FRP D VXD PDH, PDULH GH JXLVH. D GHFLIUDFDR GDV FDUWDV GH PDUB WHYH XP LPSDFWR FUXFLDO HP VHX GHVWLQR, HODV UHYHODYDP VHXV SODQRV H FRQVSLUDFRHV FRQWUD D VXA SULPD UDLQKD HOLCDEHWK SULPHLUA GA LQJODWHUUD, H IRUDP XWLOLCDGDV FRPR SURYDV LUUHIXWDYHLV HP VHX MXOJDPHQWR. DVVLP, D UHYHODFDR GH VHXV VHJUHGRV VHORX VHX GHVWLQR H FXOPLQRX HP VXA HAHFXFDR.

Desafio 7. Responda ao que se pede:

a) O que se busca proteger no recorte 1?

   Resposta: Informações confidenciais.

b) Qual o papel desempenhado pela Cifra citada no recorte 2?

   Resposta: Desempenhou o papel de precursor para os métodos modernos de criptografia.

c) Qual método foi utilizado para decifrar as mensagens da rainha do recorte 3?

   Resposta: Por meio do método de criptoanálise.

d) Como foram utilizadas as cartas decifradas da Rainha escocesa no recorte 4? E no que isso levou?

Resposta: Como provas irrefutáveis em seu julgamento, e culminou em sua execução.

Estação 3. (*Cifra de César - adaptada*) Na terceira estação os alunos precisam decifrar uma mensagem que utiliza a transposição de letras, e cifrar os seus nomes completos a partir de um dos sistemas mais conhecidos, a *Cifra de César*, que será utilizada com um deslocamento maior para o próximo desafio. Sendo assim, utilize a Tabela 4.2, em que a chave de cifração será o deslocamento de quatro posições do alfabeto original.

Tabela 4.2: Estação 3 - *Cifra de César (adaptada)*

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

Fonte: Elaborado pelo autor, 2024.

Desafio 8. Qual a sigla do Estado indicado na mensagem cifrada?

(i) Mensagem cifrada: IY REWGM IQ WES PYMW HS QEVERLES.

(ii) Mensagem decifrada: Eu nasci em São Luís do Maranhão.

Desafio 9. Utilize a Tabela 4.2 para criptografar os nomes completos de cada integrante do grupo.

Estudante 1: _____

Criptografado: _____

Estudante 2: _____

Criptografado: _____

Estudante 3: _____

Criptografado: _____

Estudante 4: _____

Criptografado: _____

Estação 4. Utilizem o mesmo princípio da Tabela 4.1, para cifrar a mensagem: A MATEMÁTICA É LINDA.

Desafio 10. A soma do valor de cifração de todas as letras utilizadas deverá ser substituída na função polinomial do 1° grau a seguir: $f(x) = \dfrac{x-3}{10}$. Qual o resultado obtido?

Resolução:

(i) Mensagem original: A MATEMÁTICA É LINDA.

(ii) Mensagem cifrada: 10362210291422102918121036143621182313 10.

(iii) Soma (total): 393. Agora, substituindo na função: $f(393) = \dfrac{393-3}{10} = 39$

Portanto, o resultado final é 39.

Desafio 11. Construam um mapa mental sobre os conhecimentos matemáticos necessários para entender a criptografia e a respeito da evolução da criptografia.

Estação 5. Os estudantes devem participar de forma individual de um jogo na plataforma *Wordwall*, chamado *Perseguição no Labirinto*. Este jogo apresentará o tema Criptografia com uma abordagem diferente, em que o nível de dificuldade e o número de vidas são determinados de acordo com o desempenho da turma. Veja, por exemplo, na Figura 4.3 uma das questões utilizadas no jogo, onde o objetivo principal é acertar a pergunta enquanto foge dos inimigos.

Figura 4.3: Perseguição no Labirinto - Wordwall

Fonte: Elaborado pelo autor, 2024.

Link do jogo: ⟨https://wordwall.net/play/77234/209/197⟩

4.1.2 Quiz

Da mesma forma, e abordando os mesmos tópicos apresentados nas atividades anteriores, os alunos participarão de um quiz desenvolvido na plataforma *Kahoot*, para aprender brincando, e, também, para verificar se estão entendo sobre os tópicos apresentados nas atividades aplicadas. Pode-se ver a tela do jogo na Figura 4.4, em que o número à esquerda representa o tempo em segundos, em contagem regressiva, para responder a questão, e o 2 a quantidade de pessoas que já responderam.

Figura 4.4: Quiz sobre Criptografia - Kahoot

Fonte: Elaborado pelo autor, 2024.

4.2 Aplicando Criptografia em sala de aula

A atividade de rotação por estações de aprendizagem foi aplicada em uma turma 8° ano e duas turmas de 9° anos para um público-alvo de 96 estudantes do Ensino Fundamental II. Assim, o processo de aplicação, iniciou-se com uma discussão sobre a parte histórica presente neste trabalho, bem como conceitos importantes para área da criptografia, tais como: codificar, decodificar, cifrar, decifrar, chaves, criptografia simétrica e assimétrica, método RSA e curvas elípticas, conforme a figura 4.5.

A abordagem do tema em sala de aula ocorreu com momentos formados por partes teóricas e práticas, e à medida que a discussão evoluía, eram propostos novos desafios para a turma, como a Cifra de César, apresentada na figura 4.6, enquanto uma parte dos estudantes precisavam decifrar frases e palavras no quadro, a outra parte resolvia numa folha impressa que lhes foram entregues. Após isso, tivemos o momento de decodificação, onde a chave era a função polinomial $y = x + 9$, em que o x é a posição das letras na sequência do alfabeto e y o resultado da codificação, conforme a tabela 4.1.

Figura 4.5: Apresentação sobre Criptografia

Fonte: Elaborado pelo autor, 2024.

Os estudantes participaram de forma ativa dos exercícios propostos, resolvendo e entendendo muito bem o funcionamento de um sistema criptográfico, principalmente na realização da decifração da Cifra de César e na decodificação dos códigos que foram solicitados a eles. Na figura 4.6, inicia-se com decifração e, após isso, a decodificação (figura 4.7), em que uma palavra codificada representa uma frase oculta. Por exemplo, calma jovem é um código utilizado pelo professor para representar férias em dezembro.

Figura 4.6: Decifração

Fonte: Elaborado pelo autor, 2024.

Figura 4.7: Decodificação em sala de aula

Fonte: Elaborado pelo autor, 2024.

No segundo encontro, em mais duas aulas de 50 minutos, foi realizada a aplicação da atividade de rotação por estações de aprendizagem na biblioteca. Os alunos tinham 5 estações de aprendizagem para passar, na Estação 1, a decifração com algarismos, e na Estação 2, a decifração com letras.

Figura 4.8: Estações 1 e 2 - Decifração

Fonte: Elaborado pelo autor, 2024.

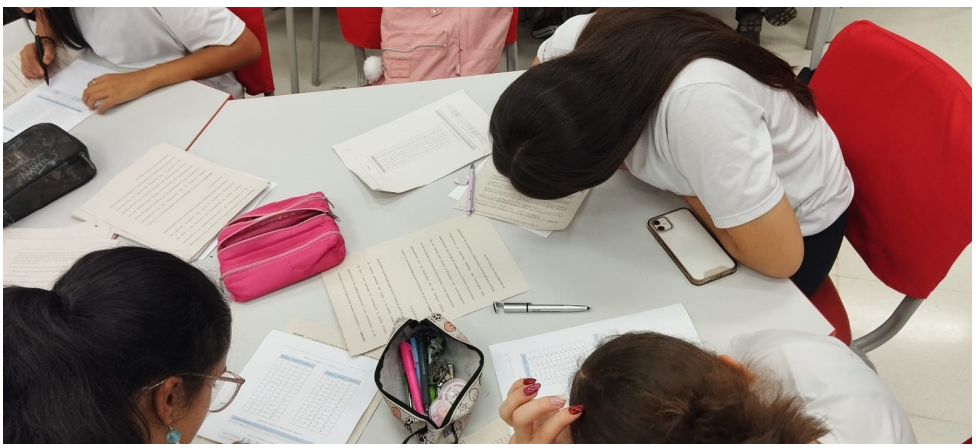
Na estação 1 era exigido dos alunos a decifração de seis frases cifradas a partir de uma chave que utiliza algarismos. No entanto, as tarefas eram mais simples, e devido a isso, muitos grupos deixaram apenas um ou dois integrantes realizando-as, enquanto outros integrantes se dirigiam a outras estações, consoante figura 4.9.

Figura 4.9: Estação 1 - Decifração da cifra com algarismos

Fonte: Elaborado pelo autor, 2024.

Na estação 2 os estudantes precisavam decifrar quatro recortes de textos que fazem parte desta dissertação, e por serem um pouco mais trabalhosos, alguns grupos, como o ilustrado na figura 4.10, dividiram-se em relação a quantidade de tarefas. Assim, cada integrante ficava com a missão de decifrar um dos recortes e, no final, juntavam-se as decifrações para finalizar a estação.

Figura 4.10: Estação 2 - Decifração da cifra com letras



Fonte: Elaborado pelo autor, 2024.

Na estação 3 era solicitado a sigla do Estado em que nasci: MA. Mas para isso era necessário decifrar uma frase criptografada, que dizia: Eu nasci em São Luís do Maranhão. Após isso, os estudantes eram desafiados a escreverem seus nomes completos na forma cifrada seguindo a tabela 4.2, e mostrado na figura 4.11.

Figura 4.11: Estação 3 - Sigla e Nome completo criptografado

Fonte: Elaborado pelo autor, 2024.

Na estação 4, enquanto alguns estudantes estavam com a missão de cifrar a frase: A MATEMÁTICA É LINDA, os outros estavam com a tarefa de construir um Mapa mental sobre Criptografia. Para a cifração, precisava-se determinar o valor da soma dos valores cifrados que foram utilizados para substituir na função polinomial: $y = \frac{x-3}{10}$. Por outro lado, para desenvolvimento do Mapa mental sobre Criptografia, era necessário realizar pesquisas e consultar o material apresentado em sala de aula.

Vale ressaltar que os estudantes do 8° ano ainda não conhecem o tema função polinomial do 1° grau, mas conseguiram desenvolver a resolução com auxílio do professor, realizando a associação da função apresentada a uma expressão algébrica, em que se busca o valor numérico. Assim, eles substituíram a soma encontrada na codificação no valor de x para encontrar o valor de y.

Na figura 4.12 é possível ver o professor orientando os alunos sobre essa "adaptação", que apesar de pequena, colabora para que estudantes consigam solucionar o problema proposto.

Figura 4.12: Estação 4 - Cifrar e Determinar o valor de y

Fonte: Elaborado pelo autor, 2024.

Na estação 5 a sugestão é aprender brincando com o jogo: Perseguição no labirinto da plataforma Wordwall, exibido na figura 4.13. Nela os estudantes colocaram em prática os conhecimentos construídos em todas as etapas aplicadas nas estações e em sala de aula, assim como, os tópicos explanados na apresentação do tema Criptografia.

No jogo ficou perceptível que os estudantes estavam se divertindo ao realizar a aprendizagem de forma prazerosa e desafiadora. Porém, para alguns grupos, ainda era necessário seguir para outras estações que não estavam concluídas, necessitando alertá-los sobre a gestão do tempo, para execução das atividades, e em relação ao tempo de permanência em cada estação, pois poderiam prejudicá-los, restando menos tempo para as próximas estações.

Figura 4.13: Estação 5 - Perseguição no Labirinto - Wordwall

Fonte: Elaborado pelo autor, 2024.

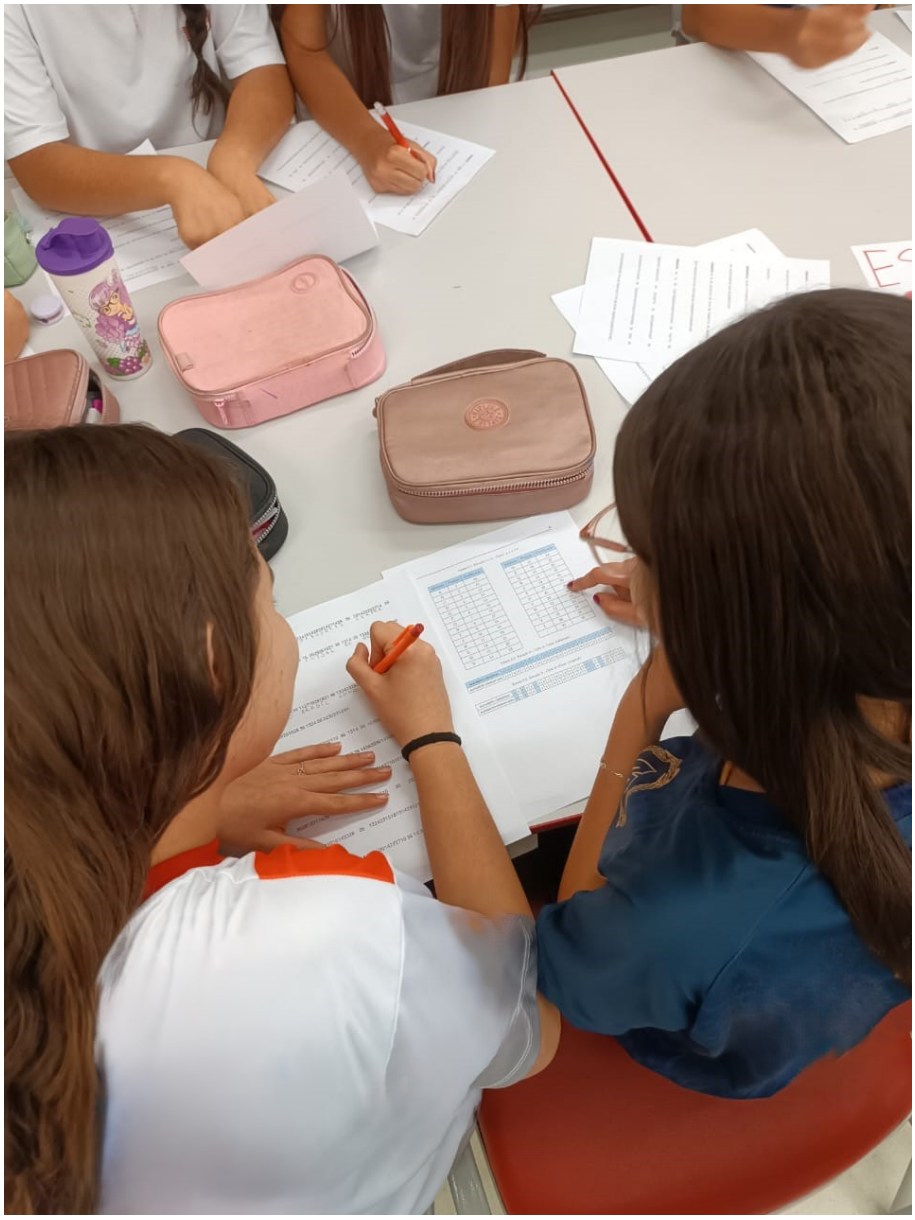
Observe na figura 4.14, que todos os estudantes se empenharam em solucionar os problemas sugeridos nas estações, dividindo as funções e tarefas para finalizar da forma mais eficiente possível.

Figura 4.14: Estudantes em ação

Fonte: Elaborado pelo autor, 2024.

Os 9° anos conseguiram se distribuir melhor nas tarefas, resolvendo os desafios um pouco mais rápido que o 8° ano. Isto ocorreu porquê distribuírem as funções de uma maneira que ficassem em duplas produtivas. Assim, enquanto um decodificada ou decifrava, o outro auxiliava na busca da correspondência e escrita, o que aumentava a eficiência e rapidez no processo de solução. Pode-se observar isso na figura 4.15.

Figura 4.15: Estudantes trabalhando em duplas



Fonte: Elaborado pelo autor, 2024.

Em relação ao jogo da Estação 5, os 9°anos quiseram ficar por bastante tempo realizando com a intenção de deixar o nome e o grupo na melhor colocação possível no ranking. No entanto, como o jogo possui apenas 21 questões, chegou um momento em que o diferencial nas posições era em relação ao tempo para finalizar o total de questões. Assim, quem acertava todas as 21 no menor tempo possível, ficava em primeiro lugar. Na figura 4.16, é possível notar uma estudante olhando o ranking dos grupos.

Figura 4.16: De olho no ranking

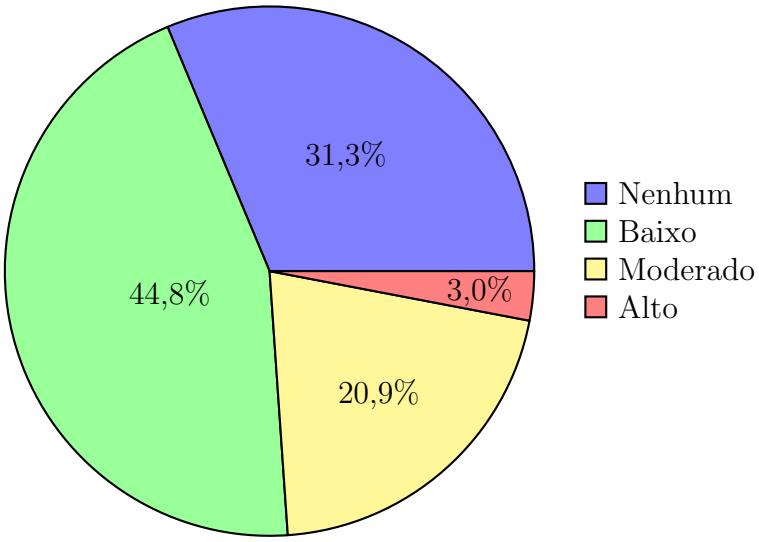
Fonte: Elaborado pelo autor, 2024.

4.3 Resultados e Discussões

Para avaliar as etapas de aplicação das atividades sobre Criptografia (apresentação teórica, jogos, estações de aprendizagem e quiz), foi sugerido um questionário para os estudantes darem seu Feedback. No entanto, dos 96 estudantes que participaram do projeto, apenas 67 estavam presentes no dia da realização do Forms.

A primeira pergunta era sobre o nível de entendimento dos alunos sobre criptografia antes da aplicação da atividade, isto é, se tinham algum conhecimento sobre o tema antes de trabalhá-lo em sala de aula. Apesar dessa questão ter sido levantada na roda de conversa em que o tema foi apresentado, aqui o objetivo era quantificar esses dados, identificando quem nunca tinha ouvido falar sobre o tema (Nenhum), quem conhecia um pouco (Baixo), e aqueles com conhecimento Moderado e Alto, conforme a figura 4.17.

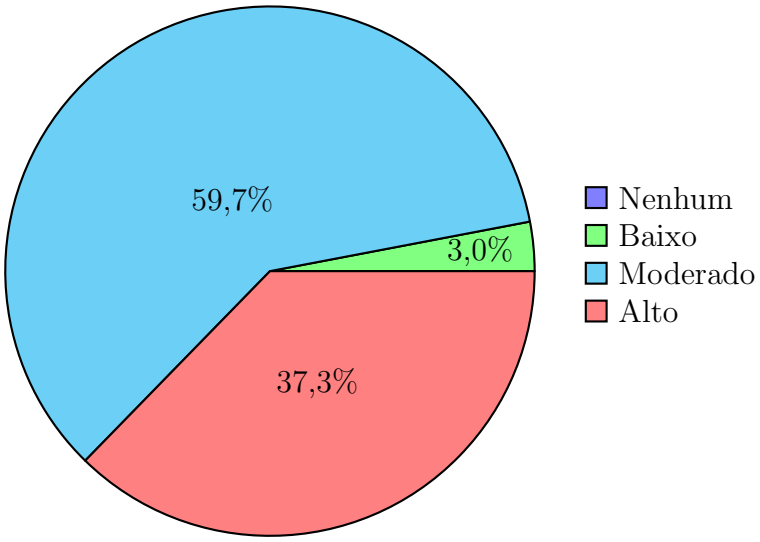
Figura 4.17: Qual era o seu nível de entendimento sobre criptografia **antes** da aplicação da atividade?



Fonte: Elaborado pelo autor, 2024.

A questão 2 trata-se sobre o nível de conhecimento sobre criptografia após a aplicação do projeto, ilustrado na figura 4.18. Note que o percentual de estudantes nos níveis Moderado e Alto subiram de forma significativa, enquanto os outros níveis caíram drasticamente, o nível Nenhum, por exemplo, diminuiu de $31,3\%$ para 0%, e o Baixo, de $44,8\%$ para 3%.

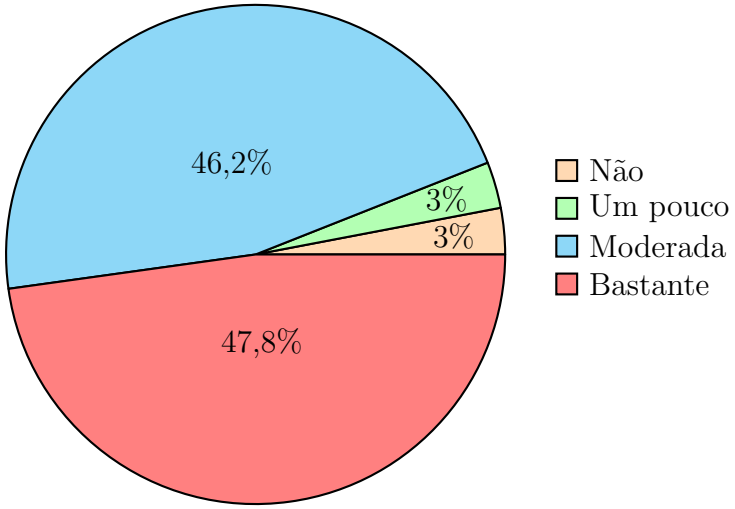
Figura 4.18: Qual é o seu nível de entendimento sobre criptografia **após** a aplicação da atividade?



Fonte: Elaborado pelo autor, 2024.

A questão 3 abordou o jogo na plataforma Wordwall, em que buscava-se entender se os alunos consideram o jogo de perseguição no labirinto uma ferramenta importante para fortalecer os conceitos aprendidos sobre criptografia. Os critérios adotados foram: não; um pouco; moderada e bastante. Pode-se observar na figura 4.19, que 97% dos alunos considera o jogo um aliado importante para fixação do conhecimento adquirido.

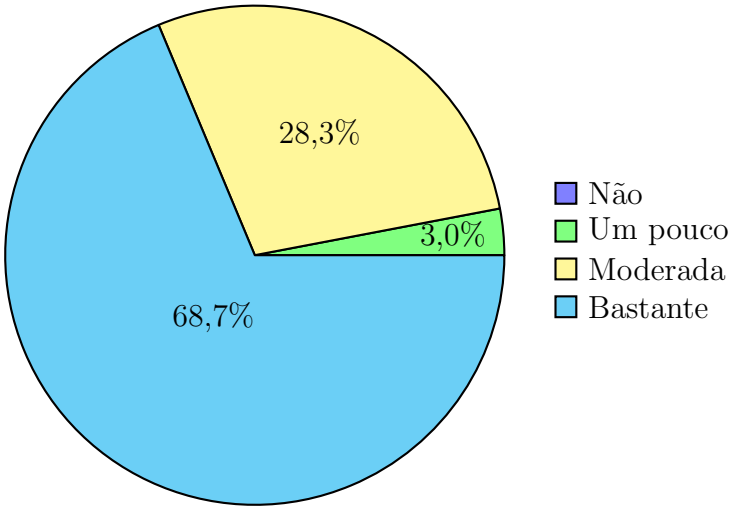
Figura 4.19: Você considera o jogo no Wordwall uma ferramenta importante para fortalecer o conceito de criptografia?



Fonte: Elaborado pelo autor, 2024.

A quarta questão refere-se ao quiz na plataforma Kahoot, cujo objetivo é verificar se os alunos estão considerando o jogo importante para a sistematização do conteúdo estudado ao longo do projeto, revisando tópicos relevantes de criptografia. Pelo gráfico apresentado na figura 4.20, nota-se que 100% dos entrevistados considera que o quiz coopera, no mínimo, um pouco para o aprendizado.

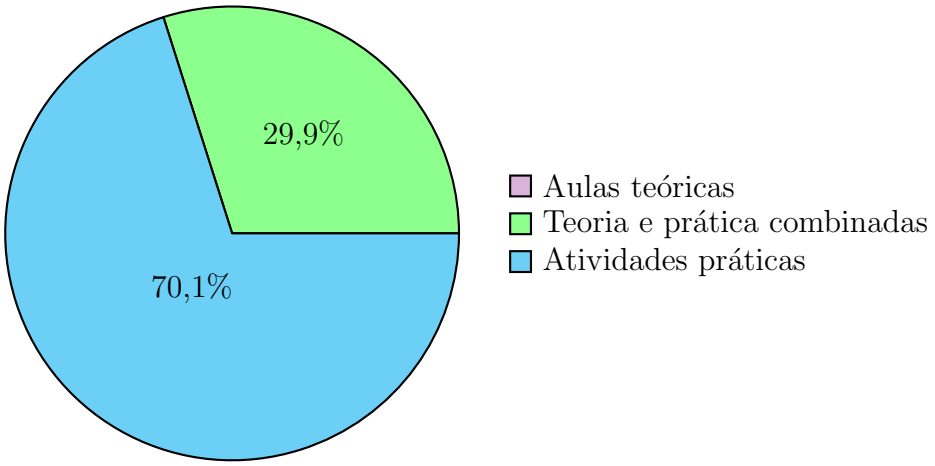
Figura 4.20: O quiz no Kahoot contribuiu para revisar os conceitos abordados nas estações?



Fonte: Elaborado pelo autor, 2024.

Na quinta pergunta, buscou-se saber se as atividades práticas, teóricas ou a combinação de ambas eram mais interessantes para os alunos. Observe na figura 4.21 que ninguém optou por aulas exclusivamente teóricas, a maioria prefere atividades práticas $(70,1\%)$, enquanto o restante escolheu a teoria aliada à prática $(29,9\%)$.

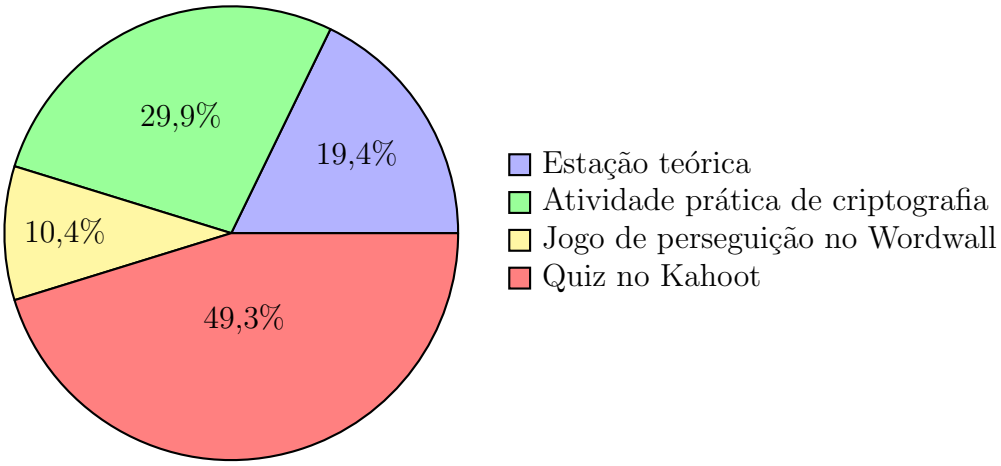
Figura 4.21: Prefere aprender através de atividades práticas, teóricas ou com a combinação de ambas?



Fonte: Elaborado pelo autor, 2024.

Com o intuito de entender em que etapa os estudantes mais aprenderam sobre criptografia, foi lançada a sexta pergunta. No gráfico da figura 4.22, observa-se que $19,4\%$ dos alunos indicaram a estação teórica, o que demonstra uma tendência a preferirem aulas diferenciadas. Também é possível perceber que uma parte considerável dos alunos considera o quiz $(49,3\%)$ importante para aprender brincando, enquanto $29,9\%$ preferem "colocar a mão na massa".

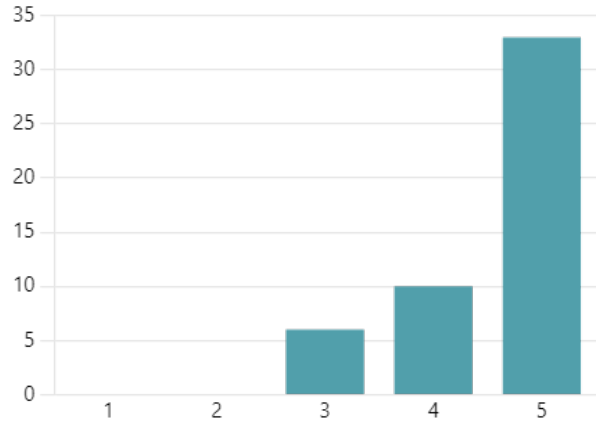
Figura 4.22: Em qual dessas atividades você percebeu que aprendeu mais sobre criptografia?



Fonte: Elaborado pelo autor, 2024.

Os discentes possuem bastante contato com jogos e novas tecnologias, e trabalhar com ferramentas educacionais que conquistem sua atenção de forma eficiente, torna-se um grande desafio. Por isso, uma sétima questão foi formulada para explorar o uso de jogos e plataformas como forma de potencializar o aprendizado, perguntando se eles acham essa abordagem interessante. Uma das plataformas utilizadas com os alunos dos 9° anos é a Khan Academy, em que trabalha-se as habilidades matemáticas que possuem defasagem. Na figura 4.23, apresenta-se um gráfico de avaliação com notas de 1 a 5 sobre o uso dessas ferramentas, e é evidente que a maioria considera essenciais para sua instrução.

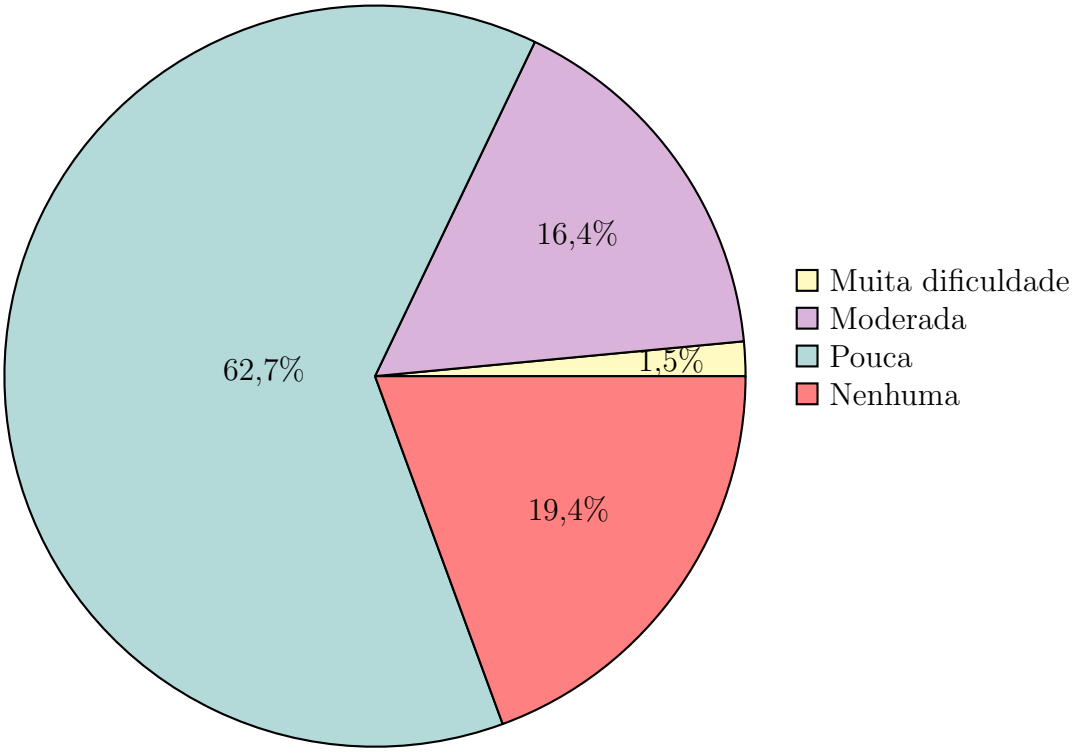
Figura 4.23: Quanto considera importante o uso de jogos e plataformas interativas para o seu aprendizado?



Fonte: Elaborado pelo autor, 2024.

No dia da apresentação das partes teórica e prática sobre criptografia em sala de aula, que precedeu a aplicação dos desafios, alguns alunos não estavam presentes. Isso comprometeu parcialmente a execução das atividades nas estações de aprendizagem aplicadas na biblioteca, pois foi necessário fornecer explicações adicionais por parte do professor e dos colegas de equipe. Diante dessas dificuldades, foi elaborada a oitava questão, com o intuito de verificar o nível de dificuldade enfrentado pelos alunos para solucionar os problemas sugeridos. Conforme apresentado na figura 4.24, $82,1\%$ dos discentes relataram pouca ou nenhuma dificuldade para resolver os problemas, enquanto $1,5\%$ relatou ter enfrentado muita dificuldade.

Figura 4.24: Qual foi o seu nível de dificuldade durante a realização das Estações de aprendizagem?



Fonte: Elaborado pelo autor, 2024.

A questão 9 perguntava: O que você aprendeu de novo sobre criptografia durante as atividades e como aplicaria esse conhecimento no seu dia a dia? Algumas das respostas foram:

A) "Os métodos utilizados, os inventores, tipos de criptografia, como fazer uma. Após o conhecimento eu vou tomar precauções ao clicar em links e imagens, desenvolveria e compartilharia este conhecimento".

B) "Aprendi tudo, já que não sabia o que era a criptografia. Acho interessante e útil para proteger informações confidenciais como dados bancários."

C) "Basicamente tudo, só sabia que criptografia era usado para proteger informações, nada mais. Acho que não vou usar em muita coisa, talvez para passar bilhetinhos sem que a fofoca seja descoberta."

D) "Eu aprendi sobre a chave e aplicaria criptografia em mensagens."

E) "Que a criptografia é importante para o dia a dia, sendo assim, a segurança."

F) 'Aprendi como funciona e aplicaria a criptografia em conversas e mensagens simples."

G) "Que a criptografia é importante para a segurança, e eu usaria para enviar uma mensagem importante."

H) "Aprendi a importância de proteger dados com criptografia. Posso usar isso criando senhas mais seguras."

I) "Eu aprendi sobre o cifra de César, a sigla RSA, o uso dela no dia a dia, a importância dela e como usar. Eu uso ela todos os dias só de mexer em eletrônicos."

Outra pergunta feita à turma: Qual parte da atividade você mais gostou? Há algo que você mudaria? A resposta da maioria dos estudantes foi que não mudariam nada, mas que gostariam de mais tempo para os jogos, "pois é uma maneira fácil e divertida de aprender", acrescentou um dos estudantes.

Em seguida, a seguinte pergunta: Você considera que o uso de jogos e plataformas interativas é importante para o seu aprendizado? Justifique sua resposta com base na experiência desta aula.

J) "Sim, é impressionante para os estudantes se descontraírem só que de uma forma que ao mesmo tempo que eles estão se divertindo, eles também estão aprendendo e reforçando o assunto."

K) "Sim, pois, como mencionei nas questões anteriores, é uma forma de fixar melhor o conteúdo, diferente das aulas teóricas que temos normalmente na sala de aula."

L) "Sim, porque é algo legal e gostaria de fazer mais."

M) “Sim, pois é uma forma de entreter e aprender de forma diferente e divertida.”

N) “Os sites e aplicativos de ensino são muito bons para pessoas com dificuldade sobre o assunto, muitos podem aprender com esses site.”

O) “Sim. Ajudou bastante a revisar e particularmente acho mais fácil de memorizar.”

P) “Sim, pois é algo que todos gostam e ajuda a compreender com mais facilidade.”

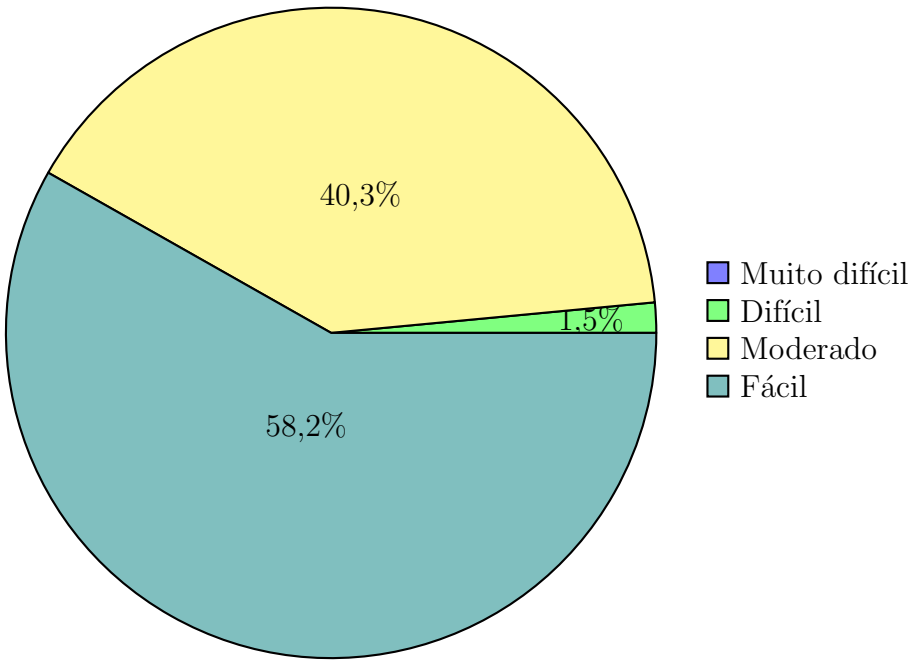
Q) “Sim, pois saímos um pouco do ambiente da sala, e distrairmos nossa cabeça.”

R) “Um pouco. Pois é um bom modo de testar nosso conhecimento e ensinar algumas coisas. Mas, na minha opinião, o modo mais eficaz é com o professor explicando.”

S) “Sim, acredito que ao decorrer do jogo consegui me lembrar bastante do que vi em sala de aula.”

A criptografia foi apresentada de forma leve para os 8° e 9° anos, retomando conceitos matemáticos, como divisibilidade, fatoração, múltiplos, números primos e decomposição em fatores primos. Sabe-se que o método RSA utiliza o processo de congruência, estudado na aritmética modular, que é geralmente abordado no ensino superior. Por isso, a parte matemática foi tratada de maneira superficial, enquanto a exploração da história, dos códigos e das cifras foi mais aprofundada, com foco em textos codificados e cifrados em tamanhos variados. A pergunta da figura 4.25 teve o objetivo de entender o nível de dificuldade da abordagem sobre criptografia, e constatou-se que a maioria dos alunos não encontrou grande dificuldade para compreendê-la.

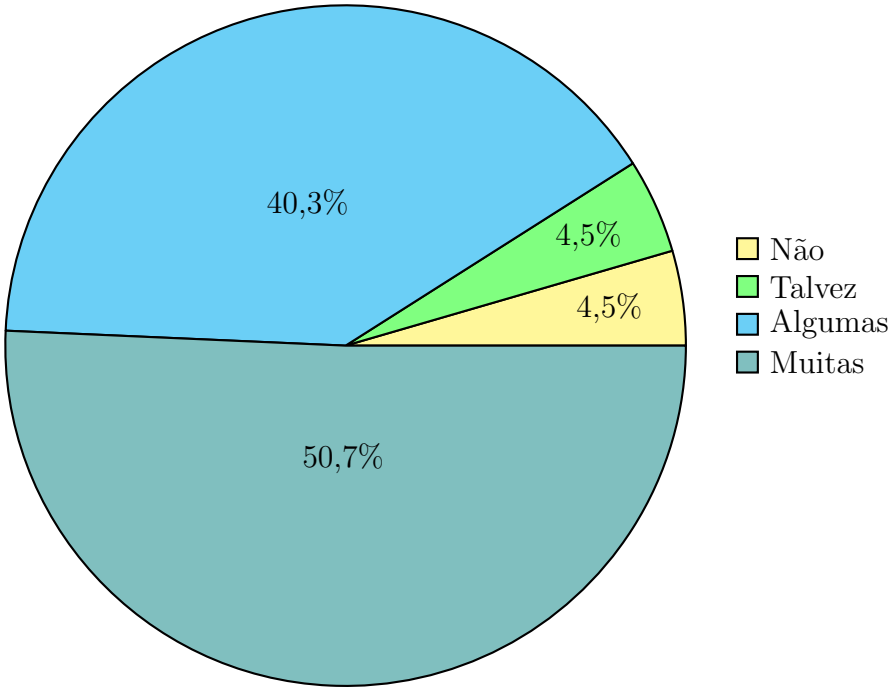
Figura 4.25: Achou o conteúdo de criptografia fácil de entender?



Fonte: Elaborado pelo autor, 2024.

A última pergunta refere-se à participação dos alunos em mais atividades semelhantes ao projeto de criptografia, mas aplicadas em outras disciplinas.

Figura 4.26: Gostaria de participar de mais atividades semelhantes em outras disciplinas?



Fonte: Elaborado pelo autor, 2024.

Como é possível constatar no gráfico da figura 4.26, 91% afirmaram que sim, gostariam de participar de projetos parecidos com outros professores. Ou seja, muitos estudantes desejam ver essa abordagem em outras matérias. Uma parceria entre vários professores, com o apoio da escola, poderia reduzir a sobrecarga sobre apenas um docente no processo de elaboração e execução dessas atividades, já que leva-se muito tempo para planejar e construir atividades, especialmente em turmas maiores, que exigem um planejamento mais detalhado e uma gestão mais rigorosa de tempo e tarefas.

Capítulo 5

Considerações Finais

Neste trabalho exploramos um pouco da história da criptografia, investigando sua evolução ao longo dos séculos, abordando códigos e cifras, e também mostrando alguns tópicos matemáticos que contribuem para a compreensão do método RSA, bem como para o método de curvas elípticas.

Com o intuito de aplicar a criptografia em sala de aula, e de mostrar o uso de alguns conhecimentos matemáticos como os números primos, foi elaborado e posto em prática um plano de aula, que iniciou-se com a retomada de temas já estudados e da elaboração de estratégias de ensino para potencializar o aprendizado, como o uso da atividade de rotação por estações de aprendizagem, jogos e quiz.

As atividades propostas surtiram um efeito positivo, pois mostraram resultados significativos, que possibilitaram ter um olhar diferenciado para novas estratégias de ensino. Acredita-se que a matemática seja muito abstrata, mas quando o professor proporciona um ambiente em que o estudante associa essa teoria a algo prático, demonstra um sentido ao que está sendo estudado, incentivando os alunos a se engajarem e, assim, contribuírem em seu processo de construção do conhecimento.

Embora muitos temas sejam difíceis de esmiuçar de forma prática durante a sua primeira discussão ou abordagem, pode-se realizar projetos ou atividades práticas como formas de sistematizar o que foi ensinado. Por exemplo, quando trabalha-se com a habilidade porcentagem, uma sugestão de atividade prática seria desenhar em folha quadriculada, conforme mencionado em jogos como estratégia de ensino neste trabalho, e visto na figura 4.2. Assim, a partir do desenho é possível trabalhar porcentagem, frações, contagem e números decimais.

Para elaboração das atividades propostas neste trabalho, um ponto importante para destacar é o tempo hábil para sua construção e concepção. Infelizmente, para a vivência do professor, é difícil ter tempo suficiente devido a quantidade de demandas do dia a dia. Por isso, sugere-se a aplicação de pelo menos um projeto a cada trimestre, como a brincadeira de torta na cara, uno (de potenciação, por exemplo), caça ao tesouro, projetos interdisciplinares, oficinas, gincanas, disputas entre turmas e outras propostas.

Apesar das adversidades que apareceram nas aplicações, como alguns erros nos recortes para decifrar, gestão do espaço e controle de tempo, a experiência é muito satisfatória, pois contribui para melhorias nas futuras aplicações nas próximas turmas, além de colaborar para o aprendizado do docente, que atua em uma busca constante por aperfeiçoamento profissional.

Em relação ao engajamento dos estudantes na execução das atividades sugeridas, nota-se a satisfação deles em aplicar os conhecimentos matemáticos e compreender o sentido dos tópicos estudados em sala. Aliás, muitas vezes, eles acham sem sentido aprender um determinado tema que, talvez, nunca usem em suas vidas, mas que, de alguma maneira, colaborarão para o desenvolvimento de seu senso crítico.

No geral, todos os alunos participaram de forma ativa, e é claro que cada um solucionou os desafios no seu próprio tempo, com alguns conseguindo resolver mais rapidamente do que outros. Além disso, o tempo, esforço e energia gastos na preparação, planejamento e execução do projeto foram dedicados com muito orgulho, e valeram a pena, pois forneceram excelentes resultados.

A maioria dos estudantes afirmaram, na pesquisa via Forms e em discussões pós aplicação, que gostaram do projeto, que querem novos desafios e que essa abordagem contribuiu muito para a construção e desenvolvimento dos saberes matemáticos, além de mostrar que as habilidades aprendidas ao longo dos anos possuem um porquê. Em virtude disso, será abordado um novo projeto sobre o tema matemática financeira, diferente do tema deste trabalho, mas fazendo uso das etapas utilizadas em sua realização.

Dessa forma, o objetivo deste trabalho foi alcançado, cumprindo-se o dever proposto e promovendo o aprendizado de novas práticas. No entanto, a pesquisa se concentrou nos métodos RSA e ECC, com maior ênfase no primeiro, principalmente devido à sua aplicabilidade em turmas do Ensino Fundamental II. Embora existam pesquisas sobre computação quântica e pós-quântica, o foco do autor foi nos métodos mais usuais e acessíveis para o contexto educacional.

Em síntese, este trabalho contribuiu para o meu desenvolvimento profissional, tanto na prática docente quanto na pesquisa acadêmica, enquanto mestrando. Espero continuar me aprimorando, desenvolvendo mais atividades e projetos que colaborem para a formação dos discentes e para o meu amadurecimento como educador e pesquisador.

Portanto, a criptografia aplicada por meio da metodologia de rotação por estações atendeu às demandas identificadas no problema de pesquisa deste projeto, proporcionando um ambiente que integra teoria e prática, onde o pensamento crítico favorece a reflexão sobre situações-problema e contribui para um trabalho colaborativo eficiente. Em relação às metas estabelecidas pela Escola, a aplicação da mesma metodologia em diferentes áreas, como a matemática financeira, resultou em uma melhora significativa nos 8^{o} e 9^{o} anos, com resultados mais expressivos observados nos 8^{o} anos.

Referências Bibliográficas

ARAUJO, R. R. de. *Reticulados algébricos e aplicações a códigos e criptografia*. 92 - 100 p. Tese (Doutorado) — Universidade Estadual de Campinas, Instituto de Matemática Estatística e Computação Científica, Campinas, SP, 2018.

ARAUJO, R. W. M. de. *Autenticação e comunicação segura em dispositivos móveis de poder computacional restrito*. Dissertação (Mestrado) — Universidade Estadual de São Paulo (USP), Instituto de Matemática e Estatística de São Paulo, 2013.

ARRUDA, T. V. de. *Análise de algoritmos paralelos de ECC em dispositivos móveis multicore*. Dissertação (Mestrado) — Programa de Pós-graduação em Ciência da Computação (PPGCCS) - Universidade Federal de São Carlos, Sorocaba, 2014.

BACICH, L.; NETO, A. T.; TREVISANI, F. d. M. *Ensino híbrido*. Porto Alegre - RS: Editora Penso, 2015. 47–80 p.

BC, B. C. do B. *O que é PIX?* Disponível em: ⟨https://www.bcb.gov.br/meubc/faqs/p/o-que-e-pix⟩. Acesso em: 21 mai. 2024.

BLOG DO WHATSAPP. *Criptografia de ponta a ponta*. 2016. Disponível em: ⟨https://blog.whatsapp.com/end-to-end-encryption?lang=pt_BR#:~:text=A%20ideia%20%C3%A9%20simples%3A%20ao,Nenhum%20hacker.⟩. Acesso em: 16 mai. 2024.

BORBA, M. D. C.; PENTEADO, M. G. *Informática e educação matemática*. Belo Horizonte: Autêntica Editora, 2019.

BOYER, C. B.; MERZBACH, U. C. *História da matemática*. 3. ed. São Paulo: Editora Blucher, 2019. 29 - 37 p.

BRERETON, G. *Introducing Assyrians. British Museum Blog*. 2018. Disponível em: ⟨https://www.britishmuseum.org/blog/introducing-assyrians⟩. Acesso em: 20 abr. 2024.

BRITISH MUSEUM. *How Egyptian hieroglyphs were decoded, a timeline to decipherment*. Disponível em: ⟨https://www.britishmuseum.org/exhibitions/hieroglyphs-unlocking-ancient-egypt/egyptian-hieroglyphs-decipherment-timeline⟩. Acesso em: 19 abr. 2024.

BRITISH MUSEUM. *Timeline of ancient Egypt*. Disponível em: ⟨https://www.britishmuseum.org/learn/schools/ages-7-11/ancient-egypt/timeline-ancient-egypt⟩. Acesso em: 19 abr. 2024.

BRUNO, O. M. *Criptografia: de arma de guerra a pilar da sociedade moderna*. 2017. Disponível em: ⟨https://jornal.usp.br/?p=63370⟩. Acesso em: 20 abr. 2024.

CARNEIRO, F. J. F. *Criptografia e Teoria dos Números*. Rio de Janeiro: Editora Ciência Moderna Ltda., 2017. v. 1.

CARVALHO, V. D. de. *Uma metodologia com uso de criptografia para ensino de funções*. Dissertação (Mestrado) — Programa de Pós-graduação em Ensino de Ciências Exatas (PPGECE) - Universidade Federal de São Carlos, Sorocaba, 2020.

COSTA, C.; FIGUEIREDO, L. M. *Introdução à Criptografia*. 3. ed. Rio de Janeiro: Repositório Institucional - CEDERJ. UFF / CEP – EB, 2010. v. 1.

COUTINHO, S. C. *Números inteiros e criptografia RSA*. Rio de Janeiro: IMPA, 2023.

D'AMBROSIO, U. *Educação Matemática: da teoria à prática*. São Paulo: Papirus Editora, 2012.

ENKVIST, I. *O complexo ofício do professor: Conselhos para uma educação de qualidade*. Campinas - SP: CEDET - Centro de Desenvolvimento Profissional e Tecnológico - Editora Kírion, 2021.

EUCLIDES. *Os elementos*. São Paulo: Unesp, 2009.

GIANNINI, A. *Cientistas descobrem segredos de Mary Stuart, rainha dos escoceses*. 2023. Disponível em: ⟨https://veja.abril.com.br/comportamento/cientistas-descobrem-segredos-de-mary-stuart-rainha-dos-escoceses⟩. Acesso em: 20 abr. 2024.

GOMES, F. R. *Um estudo exploratório envolvendo criptografia e fatoração numérica no ensino de ciências exatas*. Dissertação (Mestrado) — Programa de Pós-graduação em Ensino de Ciências Exatas (PPGECE) - Universidade Federal de São Carlos, Sorocaba, 2022.

GUITARRARA, P. *Código Morse*. 2023. Disponível em: ⟨https://brasilescola.uol.com.br/geografia/codigo-morse.htm⟩. Acesso em: 21 mai. 2024.

HEFEZ, A. *Aritmética*. 3. ed. Rio de Janeiro: Sociedade Brasileira de Matemática (SBM), 2022.

IBM, I. B. M. C. *O que é criptografia?* Disponível em: ⟨https://www.ibm.com/br-pt/topics/cryptography⟩. Acesso em: 21 mai. 2024.

LIMA, E. L. *Curso de análise: volume 1*. Rio de Janeiro: Instituto de Matematica Pura e Aplicada - IMPA, 2022.

LOUREIRO, F. O. *Tópicos de criptografia para o ensino médio*. Dissertação (Mestrado) — Universidade Estadual do Norte Fluminense Darcy Ribeiro - UENF, 2014.

MARTINELLI, L. M. B.; MARTINELLI, P. *Materiais concretos para o ensino de Matemática nos anos finais do ensino fundamental*. Curitiba: InterSaberes, 2016.

MEDEIROS, F. *Uma breve história sobre Criptografia*. 2015. Disponível em: ⟨https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/a-historia-da-criptografia/⟩. Acesso em: 18 abr. 2024.

META PLATFORMS INC. *Sobre o WhatsApp e as eleições*. Disponível em: ⟨https://faq.whatsapp.com/518562649771533?helpref=security⟩. Acesso em: 16 mai. 2024.

MORAN, J. *Educação híbrida: Um conceito-chave para a educação*. Porto Alegre - RS: Ensino híbrido: Personalização e tecnologia na educação. Penso Editora, 2015. 27–43 p.

NAKAMURA, D. *Segurança do bit menos significativo no RSA e em curvas elípticas*. Dissertação (Mestrado) — Instituto de Matemática e Estatística - USP, 2011.

NUBANK, R. *Segurança digital no Nubank: como ajudamos a te proteger*. Disponível em: ⟨https://blog.nubank.com.br/seguranca-digital-no-nubank-como-ajudamos-a-te-proteger/⟩. Acesso em: 22 mai. 2024.

OBMEP. *Sala de Estudo: Fatorando de um jeito diferente (Nível avançado)*. 2020. Disponível em: ⟨http://clubes.obmep.org.br/blog/fatorando-de-um-jeito-diferente/⟩. Acesso em: 04 jul. 2024.

OKIDA, C. M. *Protocolos de acordo de chaves baseados em emparelhamentos, para dispositivos móveis*. Dissertação (Mestrado) — Instituto de Matemática e Estatística - USP, 2011.

OLIVEIRA, M. F. de. *Um estudo sobre a implementação de criptossistemas baseados em emparelhamentos bilineares sobre curvas elípticas em cartões inteligentes de oito bits*. Dissertação (Mestrado) — Faculdade de Engenharia Elétrica e de Computação - UNICAMP, 2010.

PEREIRA, G. C. C. F. *Parametrização e otimização de criptografia de curvas elípticas amigáveis a emparelhamentos*. Dissertação (Mestrado) — Escola Politécnica - USP, 2011.

POSSIGNOLO, R. T. *Projeto de um coprocessador quântico para otimização de algoritmos criptográficos*. Dissertação (Mestrado) — Escola Politécnica - USP, 2012.

QR-CODE FÁCIL. *Gerador de QR-Code*. Disponível em: ⟨https://qrcodefacil.com/⟩. Acesso em: 21 mai. 2024.

SANTOS, G. de S. *Espaços de aprendizagem*. Porto Alegre - RS: Ensino híbrido: Personalização e tecnologia na educação. Penso Editora, 2015. 103–120 p.

SCHANKOSKI, F. R. *Criptografia e Matemática*. Dissertação (Mestrado) — Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) - Universidade Federal do Paran - UFPR, 2015.

SILVA, F. C. M. da; LIMA, A. S.; ANDRIOLA, W. B. Avaliação do suporte de tdic na formação do pedagogo. um estudo em universidade brasileira. *REICE. Revista Iberoamericana sobre Calidad, Eficacia y Cambio en Educación*, Red Iberoamericana de Investigación Sobre Cambio y Eficacia Escolar, v. 14, n. 3, p. 77–93, 2016.

SINGH, S. *O livro dos códigos*. Rio de Janeiro: Editora Record, 2001.

TRIBUNAL REGIONAL ELEITORAL - TRE. *Entenda por que não é possível fraudar a urna eletrônica*. 2024. Disponível em: ⟨https://www.tre-sp.jus.br/comunicacao/noticias/2024/Fevereiro/entenda-por-que-nao-e-possivel-fraudar-a-urna-eletronica⟩. Acesso em: 15 mai. 2024.

TRIBUNAL SUPERIOR ELEITORAL - TSE. *Entenda por que não é possível fraudar a urna eletrônica*. 2024. Disponível em: ⟨https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/criptografia⟩. Acesso em: 15 mai. 2024.

WIGGINS, G.; MCTIGHE, J. *Planejamento para a Compreensão: Alinhando Currículo, Avaliação e Ensino por Meio da Prática do Planejamento Reverso*. Porto Alegre - RS: Penso Editora, 2019. 34 - 54 p.

ZABALA, A. *A prática educativa: como ensinar*. Porto Alegre: Artmed, 2010.