UNIVERSIDADE FEDERAL DE ALAGOAS

Mestrado Profissional em Matemática em Rede Nacional
PROFMAT

DISSERTAÇÃO DE MESTRADO

A Cifra de Hill sob o olhar das planilhas eletrônicas: o estudo de matrizes aplicado à criptografia por meio do Excel.

Ana Carolina Gonçalves Araújo

Instituto de Matemática

Maceió, Fevereiro de 2026

PROFMAT

UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
- PROFMAT

ANA CAROLINA GONÇALVES ARAÚJO

A Cifra de Hill sob o olhar das planilhas eletrônicas: o estudo de matrizes aplicado à criptografia por meio do Excel.

Maceió - AL
2026

ANA CAROLINA GONÇALVES ARAÚJO

A Cifra de Hill sob o olhar das planilhas eletrônicas: o estudo de matrizes aplicado à criptografia por meio do Excel.

Dissertação de Mestrado apresentada ao Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Instituto de Matemática da Universidade Federal de Alagoas como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: *Prof. Dr. Isnaldo Isaac Barbosa*

Maceió - AL
2026

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecária Myrtes Vieira do Nascimento CRB4/1680

A663c Araújo, Ana Carolina Gonçalves.
A Cifra de Hill sob o olhar das planilhas eletrônicas: o estudo de matrizes aplicado à criptografia por meio do Excel / Ana Carolina Gonçalves Araújo. – 2026.

89 f. : il. color.

Orientação: Isnaldo Isaac Barbosa.
Dissertação (Mestrado em Matemática) – Universidade Federal de Alagoas. Instituto de Matemática. Mestrado Profissional em Matemática em Rede Nacional. Maceió, 2026.

Referências: f. 37-38.
Apêndice: f. 39-89.

1. Criptologia. 2. Cifra de Hill. 3. Álgebra linear. I. Título.

CDU: 519.6:004.056

Folha de aprovação

ANA CAROLINA GONÇALVES ARAÚJO

A Cifra de Hill sob o olhar das planilhas eletrônicas: o estudo de matrizes aplicado à criptografia por meio do Excel.

Dissertação de mestrado apresentada ao programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Alagoas, Campus A. C. Simões, como requisito parcial para a obtenção do título de Mestre em Matemática e aprovada em 23 de fevereiro de 2026.

Banca examinadora:

gov.br Documento assinado digitalmente
ISNALDO ISAAC BARBOSA
Data: 13/05/2026 11:19:37-0300
Verifique em https://validar.iti.gov.br

Orientador: Prof. Dr. Isnaldo Isaac Barbosa
(Universidade Federal de Alagoas)

gov.br Documento assinado digitalmente
MARCOS RANIERI DA SILVA
Data: 11/05/2026 15:14:29-0300
Verifique em https://validar.iti.gov.br

Examinador Interno: Prof. Dr. Marcos Ranieri da Silva
(Universidade Federal de Alagoas)

gov.br Documento assinado digitalmente
DANIEL NICOLAU BRANDAO
Data: 13/05/2026 10:12:24-0300
Verifique em https://validar.iti.gov.br

Examinador Externo: Prof. Dr. Daniel Nicolau Brandão
(Universidade Estadual de Alagoas)

Ao meu primeiro professor de Matemática,
Marcelo Araújo, meu Pai.

AGRADECIMENTOS

Agradeço a Deus, por ter sonhado com esse tempo na minha vida muito antes de mim, ter me ensinado a sonhar junto e ter me mostrado que, nesse tempo, o mestrado era um detalhe no meio da grandiosidade do caminho.

À minha mãe, Simone Gonçalves, minha primeira e eterna professora, por me dar a vida e estar sempre ao meu lado. E ao meu pai, Marcelo Araújo, por que ainda lembro de todas as vezes que chegava cansado do trabalho, depois de passar o dia ensinando Matemática e ainda tinha disposição para me ensinar a dividir, os números e a vida.

Às minhas avós, Gelva Gonçalves e Maria das Graças Araújo (in memoriam) por ainda viverem todos os dias em minha memória e no meu coração.

Ao meu irmão, Matheus Araújo, por ser a minha pessoa favorita nesse mundo. E ao meu irmãozinho, Lucas Lima, porque, por mais que ainda esteja longe de entender algo sobre matrizes, espero que a Matemática o encontre assim como encontrou a mim e ao Matheus.

Aos amigos e colegas do PROFMAT, em especial aos "Zumbis do PROFMAT", em ordem alfabética: Álvaro Raonny, Everton Laurentino, Misael Lins, Pedro Fidelis, Petrucío Sobeira, Symon Pinheiro, Vanessa Ferreira e Vinícius Sabino. Obrigada por compartilharem comigo todas as felicidades e dificuldades da vida de mestrandos e por todos os outros momentos extraordinários que vivemos. Não teriam sido anos tão incríveis sem a parceria de vocês, Mestres.

À minha primeira família em Maceió, as "mestras interestaduais"e amigas que aguardaram pacientemente por esse momento, por sempre estarem dispostas a me ouvir, aconselhar e apoiar, também em ordem alfabética: Anny Lopes, Luana Gregório, Paula Lima e Rebeca Santana.

À nova família maceioense da minha vida, o Sinai, por cada intercessão silenciosa por mim, pela vida cristã e por essa dissertação. Obrigada por serem lar em meio a tantas novidades.

Ao meu orientador, Prof. Dr. Isnaldo Isaac Barbosa, por cada cuidado prestado desde o Exame de Qualificação, por todo tempo e interesse dedicados para a realização deste trabalho e pela paciência em meio ao turbilhão. Sou eternamente grata por todo seu apoio.

Sou grata também a todos os outros professores que compõem o colegiado do PROFMAT e um agradecimento especial aos professores que lecionaram disciplinas durante estes anos de mestrado: Adina Rocha, André Flores, Carlos Gonçalves, Cláudia Lozada, Gregório Neto, José Anderson de Lima, Marcos Ranieri e Vânio Fragoso. Sou grata por cada ensinamento e tempo dedicados.

Por fim, agradeço à banca examinadora, Prof. Dr. Marcos Ranieri e Prof. Dr. Daniel Nicolau Brandão, pelo tempo dedicado à minha pesquisa e pelas contribuições feitas.

Derrubai as barreiras da superficialidade e do medo! Reconhecendo-vos como homens e mulheres novos, regenerados pela graça batismal.

— SÃO JOÃO PAULO II

RESUMO

Diante dos desafios enfrentados pela Educação Básica, especialmente no Ensino Médio, torna-se cada vez mais necessário buscar estratégias que promovam o engajamento dos estudantes e atribuam significado aos conteúdos matemáticos trabalhados em sala de aula. Nesse contexto, a criptografia apresenta-se como uma temática potencialmente rica para o ensino contextualizado, ao articular conceitos matemáticos a aplicações presentes na sociedade contemporânea. Dessa forma, este trabalho aplica o uso da Cifra de Hill como recurso didático para o ensino de Matrizes e Determinantes no Ensino Médio, explorando seus fundamentos matemáticos e sua implementação por meio de planilhas eletrônicas. Inicialmente, é apresentado um breve panorama histórico da criptografia, destacando sua evolução ao longo do tempo. Em seguida, são apresentados os conceitos matemáticos envolvidos na Cifra de Hill, tais como operações com matrizes, determinantes, invertibilidade e aritmética modular, com abordagem através de processo exemplificado. Como desdobramento da proposta, desenvolveu-se um produto educacional constituído por um conjunto de planilhas no software Excel (em sua versão online), que automatizam os processos de codificação e decodificação da Cifra de Hill. Essas planilhas foram criadas de modo a explicitar as etapas matemáticas do algoritmo criptográfico, focando na visualização dos procedimentos e na compreensão conceitual dos conteúdos envolvidos, sem substituir o raciocínio matemático. Dessa forma, o trabalho busca contribuir para a prática docente ao apresentar uma alternativa metodológica que integra Matemática, tecnologia e criptografia, possibilitando uma abordagem mais contextualizada e significativa para o ensino de Matrizes e Determinantes no Ensino Médio.

Palavras-chave: Criptografia; Cifra de Hill; Matrizes; Determinantes; Excel.

ABSTRACT

Given the challenges faced by Basic Education, especially in High School, it becomes increasingly necessary to seek strategies that promote student engagement and attribute meaning to the mathematical content worked on in the classroom. In this context, cryptography presents itself as a potentially rich topic for contextualized teaching, as it connects mathematical concepts to applications present in contemporary society. Thus, this work applies the use of the Hill Cipher as a didactic resource for teaching Matrices and Determinants in High School, exploring its mathematical foundations and its implementation through spreadsheets. Initially, a brief historical overview of cryptography is presented, highlighting its evolution over time. Then, the mathematical concepts involved in the Hill Cipher are presented, such as operations with matrices, determinants, invertibility, and modular arithmetic, with an approach through an exemplified process. As a follow-up to the proposal, an educational product was developed, consisting of a set of Excel spreadsheets (online version), that automate the encoding and decoding processes of the Hill Cipher. These spreadsheets were created in order to explain the mathematical steps of the cryptographic algorithm, focusing on visualizing the procedures and understanding the conceptual content involved without replacing mathematical reasoning.Therefore, this work seeks to contribute to teaching practice by presenting a methodological alternative that integrates Mathematics, technology, and cryptography, enabling a more contextualized and meaningful approach to teaching Matrices and Determinants in High School.

Keywords: Cryptography; Hill Cipher; Matrices; Determinants; Excel.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Dentre todos os desafios encontrados diariamente pela Educação Básica Brasileira, a evasão escolar tem se destacado, especialmente no que tange à etapa do Ensino Médio. Silva (2021) expõe que dentre os anos de 2011 e 2019, O Ensino Médio Alagoano teve taxas de abandono maiores que as do Nordeste e do Brasil e que, embora tenha melhorado um pouco após essa época a partir da adoção de políticas públicas educacionais como o programa "Escola 10", ainda há disparidade entre esses índices educacionais. Nesse contexto do Ensino Médio, a evasão escolar está associada a diversos fatores, entre esses, encontram-se estudantes desmotivados e desinteressados, por vezes com esses sentidos motivados por currículos extensos e desconexos com sua realidade, fator relevante de desmotivação e abandono escolar, (Araújo *et al.*, 2025).

No entanto, esses mesmos alunos encontram-se como observadores e participantes de um mundo em constante transformação tecnológica. Esse contexto pode e deve ser usado a favor da Educação Básica, especialmente no que se refere a Educação Matemática, articulando saberes tradicionais ao uso de novas ferramentas digitais. Essas ferramentas digitais podem ser alternativas para ministrar os conceitos teóricos trabalhados na matemática e para realizar aulas que estimulem os estudos de forma mais significativa, além de propiciar aos educandos técnicas para a resolução de problemas não possíveis com papel e caneta (Lima *et al.*, 2022).

Nesse cenário, a criptografia desponta como uma temática potencialmente rica para o ensino contextualizado de diversos conteúdos matemáticos, ao mesmo tempo em que estimula o uso de tecnologias digitais na resolução de problemas envolvendo cifras e códigos (Kranz *et al.*, 2024). Conforme defendem Groenwald *et al.* (2007), a integração da Matemática com outros campos do saber torna o processo de ensino mais interessante e motivador, abrindo espaço para abordagens interdisciplinares e metodologias inovadoras que atribuem maior significado à aprendizagem.

À luz dessas discussões, esta dissertação apresenta uma proposta de uso da Criptografia, por meio da Cifra de Hill, como recurso didático para o estudo de Matrizes e Determinantes no Ensino Médio. A escolha pela Cifra de Hill justifica-se por sua natureza essencialmente matemática, uma vez que esse sistema criptográfico utiliza operações com matrizes para realizar substituições polialfabéticas, permitindo uma abordagem conceitual consistente dos conteúdos envolvidos (Brandão, 2017). Além disso, trabalhos anteriores apontam o potencial da temática criptográfica para o ensino de matrizes no Ensino Médio, reforçando sua pertinência pedagógica.

O objetivo geral deste trabalho é investigar o uso da Cifra de Hill como recurso didático para o ensino de Matrizes e Determinantes, por meio do desenvolvimento de um produto educacional. Como objetivos específicos, busca-se implementar a Cifra de Hill na criação de uma interface utilizando o software Excel, bem como elaborar propostas de práticas educacionais que articulem esse recurso tecnológico à prática docente.

Para a implementação da proposta, foram exploradas funcionalidades do Excel que possibilitam a automação de cálculos matriciais e a simulação de codificações criptográficas, visando proporcionar uma experiência prática e visual do conteúdo, permitindo que os estudantes compreendam conceitos como multiplicação de matrizes, determinantes e matrizes inversas, ao mesmo tempo em que experimentam uma aplicação concreta da Matemática. Como desdobramento pedagógico, foi elaborado um material de apoio ao professor, intitulado *Cifrando*

Matrizes e Decifrando Segredos, contendo orientações metodológicas e propostas de atividades contextualizadas.

1. UM BREVE RELATO HISTÓRICO ACERCA DA UTILIZAÇÃO E IMPORTÂNCIA DA CRIPTOGRAFIA

Esta abordagem relata o princípio histórico da criptografia, sendo utilizada como instrumento de guerra, até os dias atuais, em que a criptografia ganhou força na utilização das estruturas de sites para compras online e como integrante dos métodos de segurança de dados bancários.

1.1. A criptografia na Era Medieval

Na história da origem das civilizações existem várias passagens onde havia trocas de mensagens secretas, principalmente em períodos de guerras, o intuito era que o inimigo não tivesse acesso a informações especiais sobre suas táticas de guerra. O autor Singh (2022) em seu livro: O livro dos códigos, apresenta a história intitulada: O código de Maria, rainha da Escócia, que se passa em 15 de outubro de 1586, no castelo de Fotheringhay, onde a rainha Maria estava sendo acusada de planejar junto a outros membros da corte, a morte da rainha Elisabeth I, a fim de ocupar o seu lugar no trono da Inglaterra.

> Na manhã de seu julgamento, Maria estava sozinha no banco dos réus, usando um vestido preto de luto. Em caso de traição, o acusado não tinha direito a advogado e nem podia convocar testemunhas. Maria não contara nem mesmo com a ajuda dos secretários para ajudá-la a preparar uma defesa. Contudo percebia que sua situação não era sem esperanças, porque fora cuidadosa em garantir que toda a sua correspondência com os conspiradores fosse escrita em linguagem cifrada. As cifras tinham transformado suas palavras em uma série de símbolos sem sentido. Maria acreditava que, mesmo se Walsingham tivesse se apoderado das cartas, não poderia decifrar as palavras que continham. E se o conteúdo era um mistério, então as cartas não poderiam ser usadas como prova contra ela. Tudo dependia da suposição de que a cifra não fora quebrada (Singh, 2022).

Walsingham, era primeiro-secretário e chefe da espionagem inglesa, ele interceptou as cartas de Maria aos conspiradores e conhecia Thomas Phelippes, o maior especialista em decifrar códigos. O autor não entra no detalhe do resultado do julgamento, mas sabe-se pela História que a rainha Maria foi decapitada em 1587, por causa da sua traição contra Elisabeth I.

Nesta mesma obra, Singh (2022) analisa as causas e os acontecimentos dos conflitos entre gregos e persas, as comumente conhecidas "Guerras Médicas"do século V a.C). Enfatizando o contraste cultural entre as duas civilizações em guerra: a Pérsia tendo obediência ao rei como um dos seus pilares e um vasto império multicultural, e a Grécia composta por cidades-estados independentes, valorizando a liberdade política e a participação cívica. Neste contexto ele conta que, em alguns momentos mensagens codificadas foram enviadas a fim de que o adversário não soubesse do conteúdo, pois quando Xérxes, o rei da Persia, construiu uma cidade, Persépolis, a

inimizade entre Grécia e Pérsia aumentou e Xérxes planejava um ataque à Grécia. No entanto, havia um Grego ao lado dos Persas, o Demerato, que ao ficar sabendo do ataque planejou avisar a Grécia enviando uma mensagem de modo que os Persas não conseguissem decifrá-la.

> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os outros gregos (Singh, 2022).

Este é um relato importante para evidenciar a necessidade de esconder as mensagens verdadeiras no caso de posse dos inimigos, Xérxes perdera o elemento vital da surpresa, e, quando a frota persa se aproximou da baía de Salamina, perto de Atenas, os Gregos estavam preparados. Essa comunicação secreta, obtida através da ocultação da mensagem, é conhecida como *esteganografia*, nome derivado das palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever.

> Portanto, em paralelo com o desenvolvimento da esteganografia, houve a evolução da criptografia, derivada da palavra grega kriptos, que significa "oculto". O objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado - um processo conhecido como encriptação (Singh, 2022).

Os primeiros casos de mensagens realmente criptografadas, isto é, informações transformadas em outras, caracterizam o que hoje é conhecido por "criptografia clássica"que é subdividida em dois ramos: criptografia de transposição e criptografia de substituição. Martíns (2023) comenta que:

> As transposições (ou simétricas) simplesmente mudam-se ou permutam-se as letras de uma mensagem, de acordo com um padrão e uma chave previamente estabelecida entre o remetente e o destinatário. Nas substituições (ou assimétricas) as letras da mensagem original são trocadas por outras. Podendo ser monoalfabéticas quando não depende da letra na mensagem, isto é, cada letra do texto original é representada por qualquer posição pela mesma substituta, ou polialfabéticas quando depende da letra original e da sua posição no texto.

Isto é, na transposição a base é a permutação entre as letras, o que não garante segurança, pois informações pequenas têm poucas possibilidades de rearranjamento, embora, devido a esse mesmo aspecto, mensagens grandes levem mais tempo e, portanto, aparentem segurança no sigilo. A substituição pode, então, ser uma aliada ao objetivo da criptografia clássica, pois "Em alguns algoritmos, utiliza-se uma combinação entre as cifras de substituição e as de transposição, dificultando um pouco mais a decodificação da mensagem"(Cavalcante, 2009).

Além destas, existem várias histórias do uso da codificação em mensagens, mas todas elas e o avanço da ciência e, principalmente, da tecnologia, apontam sempre na direção da necessidade urgente da humanidade na articulação e uso de dados criptografados.

1.2. A criptografia na Atualidade

Devido às contribuições históricas, há uma diversa gama de métodos e cifras criptográficas, desenvolvidas por diversos atores da humanidade. Alguns desses ainda muitos utilizados, outros nem tanto, mas todos eles contribuíram para que a criptografia evoluísse a ponto de tornar-se segura o suficiente para a humanidade usá-la em todos os tipos de atividades financeiras e de segurança. (Aravéchia; Dian, 2024), ao falarem sobre um método antigo de criptografia, o RSA, que é utilizado até hoje, apontaram que esse uso se dá devido a maturidade que o algoritmo ganha com o tempo, fortificada através dos diversos testes realizados, entrando em conhecimento os pontos fortes do método, dificultando falhas catastróficas na utilização.

> Na era moderna, com o advento da computação e grandes quantidades de dados que precisam ser protegidos, a criptografia atual é muito mais complexa do que as cifras de substituição utilizadas por boa parte da história, utilizando-se agora de teorias e operações matemáticas complexas e suposições de dureza computacional, projetando algoritmos computacionalmente seguros, em que apesar de em teoria seja possível quebrá-los, na prática, a demanda computacional para se realizar isso impossibilita que isso aconteça (Almeida, 2025).

Dentre as utilizações dos algoritmos de criptografia mais atuais, alguns deles que utilizam-se, inclusive, de tecnologia quântica, destacam-se o uso de criptografia de ponta por instituições de comércio online e bancos, que usam a criptografia pela necessidade de proteger dados financeiros e pessoais dos clientes, garantir a segurança das transações, transformando informações sensíveis como senhas, números de conta e dados de cartões em códigos que só sistemas autorizados conseguem ler. Ela é aplicada tanto no armazenamento dessas informações quanto na transmissão pela internet, como no uso de apps e internet banking, impedindo que terceiros interceptem ou entendam os dados, além de ajudar a prevenir fraudes e cumprir leis e normas de segurança. Como concordam Monfre *et al.* (2023) ao dizerem que:

> No ambiente digital atual, a criptografia é amplamente utilizada para garantir a confidencialidade, integridade e autenticidade de dados em múltiplas plataformas. Sistemas ban-

> cários, e-commerces, serviços de saúde, redes sociais e governos dependem de sistemas criptográficos para garantir a proteção de seus ativos informacionais

Os autores Monfre *et al.* (2023) ainda citam a presença da criptografia nos debates éticos e políticos, fruto do grande papel e espaço tomado por essa ciência nos meios humanos, citando paradigmas entre liberdade individual e responsabilidade coletiva.

Diante desse panorama, que evidencia a evolução da criptografia desde práticas rudimentares até sistemas altamente sofisticados e tecnologicamente avançados, torna-se pertinente refletir sobre como esse campo do conhecimento pode ser explorado no contexto educacional. Embora os algoritmos modernos envolvam estruturas matemáticas complexas e tecnologias avançadas, é possível identificar métodos criptográficos clássicos que, mesmo sendo historicamente anteriores, mantêm relevância pedagógica por se apoiarem em conceitos matemáticos acessíveis ao Ensino Médio. Nesse sentido, a Cifra de Hill destaca-se por utilizar matrizes, determinantes e aritmética modular, conteúdos previstos nos currículos dessa etapa de ensino, constituindo-se como uma alternativa didática que permite articular história, tecnologia e Matemática de forma contextualizada. Essa abordagem possibilita não apenas a compreensão de fundamentos matemáticos, mas também a aproximação dos estudantes a aplicações concretas da criptografia, tema que permeia de maneira significativa a sociedade contemporânea.

2. FUNDAMENTOS MATEMÁTICOS DA CIFRA DE HILL

A Cifra de Hill constitui uma ferramenta de natureza matemática que, enquanto processo de criptografia baseado em matrizes e determinantes, apresenta-se como uma aliada para o ensino e a aprendizagem desses conteúdos no Ensino Médio, uma vez que possibilita a articulação entre objetos matemáticos estudados e situações-problema contextualizadas. Nesse sentido, este capítulo tem como objetivo apresentar os fundamentos matemáticos necessários à compreensão da Cifra de Hill, de modo a subsidiar as atividades propostas no produto educacional apresentado no Anexo A desta dissertação.

A abordagem adotada baseia-se na codificação e decodificação de uma mensagem, a partir da qual são discutidos, de forma progressiva e didática, conceitos como representação alfanumérica, organização em blocos, escolha da matriz-chave, operações com matrizes e a relação entre determinante e invertibilidade. Ressalta-se que a exposição privilegia um nível conceitual adequado ao Ensino Médio, com ênfase em aspectos relevantes para a prática docente.

2.1. O estudo de Matrizes e Determinantes no livro didático do Ensino Médio

No contexto do Ensino Médio, o livro didático constitui um dos principais referenciais para a abordagem dos conteúdos matemáticos, influenciando tanto a seleção quanto a forma de apresentação dos temas trabalhados em sala de aula. Conforme Andrade (2024), o livro didático é amplamente utilizado como recurso presente na realidade escolar, atuando como elo entre os parâmetros curriculares e o trabalho dos professores de Matemática em sala de aula.

Diante disso, considerando a estreita relação entre o livro didático e as práticas docentes, adota-se como referência, para ilustrar o cenário atual, o livro didático Bonjorno *et al.* (2020), amplamente utilizado em escolas estaduais de Alagoas.

O conteúdo de Matrizes é apresentado no primeiro capítulo do módulo "Sistemas, Matemática Financeira e Grandezas"e tem como foco os tópicos indicados em seu sumário (ver Figura 2.1). Nesse contexto, são abordados inicialmente conceitos introdutórios, como a definição de matriz, incluindo a matriz quadrada, bem como a noção de igualdade entre matrizes. Em seguida, o estudo concentra-se nas operações básicas envolvendo matrizes, tais como adição, subtração e multiplicação, enfatizando procedimentos algorítmicos e técnicas de cálculo. A abordagem adotada pelo material prioriza a apresentação de exemplos resolvidos, seguidos de listas de exercícios, com o objetivo de consolidar as técnicas operatórias relacionadas a esses conteúdos.

Contudo, é fundamental compreender que essa estrutura do livro não esgota as possibilidades pedagógicas, já que "nenhum livro didático, por melhor que seja, pode ser utilizado sem adaptações". A autora reitera que, "como todo e qualquer livro, o didático também propicia diferentes leituras para diferentes leitores"(Lajolo, 1996). Cabendo ao professor o papel de mediador para que essa ferramenta dialogue efetivamente com a realidade específica de sua

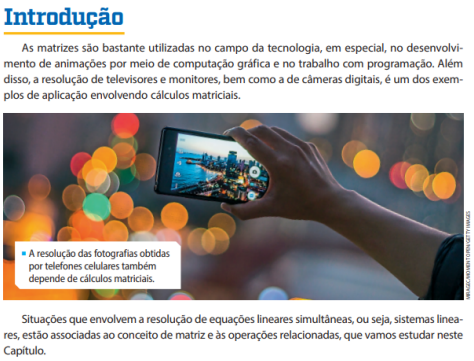
turma."

Figura 2.1 Sumário do capítulo sobre Matrizes do Livro Didático

Conforme ilustrado na Figura 2.2, o conteúdo de matrizes é introduzido no livro didático por meio de exemplos de aplicação relacionados à tecnologia, como a resolução de imagens digitais e o uso de dispositivos eletrônicos. A abordagem inicial busca evidenciar a presença das matrizes em situações do cotidiano, porém sem aprofundar, nesse momento, a relação entre essas aplicações e os conceitos matemáticos que serão desenvolvidos ao longo do capítulo, os quais passam a ser tratados posteriormente de forma mais formal e procedimental. No entanto, essa abordagem inicial concorda com Ferreira *et al.* (2025) ao afirmarem que a matemática

pode promover engajamento no processo de ensino e aprendizagem, em especial, quando é associada ao uso de tecnologias da informação e comunicação.

Figura 2.2 Introdução do capítulo sobre Matrizes do Livro Didático


Introdução

As matrizes são bastante utilizadas no campo da tecnologia, em especial, no desenvolvimento de animações por meio de computação gráfica e no trabalho com programação. Além disso, a resolução de televisores e monitores, bem como a de câmeras digitais, é um dos exemplos de aplicação envolvendo cálculos matriciais.

A resolução das fotografias obtidas por telefones celulares também depende de cálculos matriciais.

Situações que envolvem a resolução de equações lineares simultâneas, ou seja, sistemas lineares, estão associadas ao conceito de matriz e às operações relacionadas, que vamos estudar neste Capítulo.

Essa aplicação sugerida no texto introdutório volta a ser resgatada em alguns tópicos e exercícios nas seções do próprio livro didático, ressaltando-se, aqui, dois exercícios que fazem referência à criptografia com a Cifra de Hill e que levam o estudante a transformar mensagens em matrizes ou, então, a operar com matriz para decodificar uma mensagem. Observe essas duas questões nos Exemplos 2.1.1 e 2.1.2.

Exemplo 2.1.1. *(Atividade 1, p. 17, Bonjorno et al. (2020)) (Unimontes-MG) Ao associarmos as letras do alfabeto aos números, segundo a correspondência*

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

podemos afirmar que a palavra UNIMONTES pode ser codificada pela matriz 3 x 3 dada por:

a. $\begin{bmatrix} 21 & 14 & 9 \\ 13 & 15 & 14 \\ 19 & 5 & 20 \end{bmatrix}$;

b. $\begin{bmatrix} 21 & 14 & 9 \\ 13 & 15 & 14 \\ 20 & 5 & 19 \end{bmatrix}$;

c. $\begin{bmatrix} 21 & 14 & 9 \\ 13 & 16 & 14 \\ 20 & 5 & 19 \end{bmatrix}$;

d. $\begin{bmatrix} 21 & 14 & 9 \\ 13 & 16 & 14 \\ 19 & 5 & 20 \end{bmatrix}$.

Resposta. Essa atividade é reforço do conteúdo de definição de Matriz e consiste na simples transição de letras para números e na organização destes em blocos de 3 elementos dispondo, posteriormente, cada bloco como vetor linha de uma matriz. Sendo assim,

$$U \to 21,\ N \to 14,\ I \to 9$$
$$M \to 13,\ O \to 15,\ N \to 14$$
$$T \to 20,\ E \to 5,\ S \to 19$$

Gerando, assim, a matriz:

b. $\begin{bmatrix} 21 & 14 & 9 \\ 13 & 15 & 14 \\ 20 & 5 & 19 \end{bmatrix}$

Exemplo 2.1.2. *(Atividade 5, p. 26, Bonjorno et al. (2020)) (UFPB) As mensagens entre duas agências de espionagem, Gama e Rapa, são trocadas usando uma linguagem de códigos, onde cada número inteiro entre 0 e 25 representa uma letra, conforme mostra a tabela a seguir:*

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

A agência Gama enviou para a Rapa o nome de um espião codificado na matriz

$$A = \begin{bmatrix} 11 \\ 1 \\ 0 \\ 0 \\ 2 \end{bmatrix}.$$

Para decodificar uma palavra de cinco letras, dada por uma matriz A, de ordem 5 x 1, formada por inteiros entre 0 e 25, deve-se multiplicá-la pela matriz de conversão

$$\begin{bmatrix} 1 & 9 & 0 & 0 & 0 \\ 0 & 3 & 5 & 20 & 2 \\ 0 & 0 & 0 & 0 & 7 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 3 \end{bmatrix}$$

e, usando-se a tabela dada, converter os números em letras. Utilizando-se esse processo, conclui-se que o nome do espião é:

a. *DIEGO*

b. *SHUME*

c. SADAN

d. RENAN

e. RAMON

Resposta. Nesta atividade o livro já entrega uma mensagem codificada em uma matriz coluna com 5 linhas e uma matriz de decodificação de ordem 5. Bastando, ao estudante, multiplicar ambas as matrizes e reorganizar a mensagem utilizando uma tabela de referência. Assim,

$$\begin{bmatrix} 1 & 9 & 0 & 0 & 0 \\ 0 & 3 & 5 & 20 & 2 \\ 0 & 0 & 0 & 0 & 7 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 1 \\ 0 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 1\cdot 11+9\cdot 1+0\cdot 0+0\cdot 0+0\cdot 2 \\ 0\cdot 11+3\cdot 1+5\cdot 0+20\cdot 0+2\cdot 2 \\ 0\cdot 11+0\cdot 1+0\cdot 0+0\cdot 0+7\cdot 2 \\ 0\cdot 11+1\cdot 1+0\cdot 0+0\cdot 0+0\cdot 2 \\ 0\cdot 11+2\cdot 1+0\cdot 0+0\cdot 0+3\cdot 2 \end{bmatrix} =$$

$$= \begin{bmatrix} 1\cdot 11+9\cdot 1+0\cdot 0+0\cdot 0+0\cdot 2 \\ 0\cdot 11+3\cdot 1+5\cdot 0+20\cdot 0+2\cdot 2 \\ 0\cdot 11+0\cdot 1+0\cdot 0+0\cdot 0+7\cdot 2 \\ 0\cdot 11+1\cdot 1+0\cdot 0+0\cdot 0+0\cdot 2 \\ 0\cdot 11+2\cdot 1+0\cdot 0+0\cdot 0+3\cdot 2 \end{bmatrix} =$$

$$= \begin{bmatrix} 11+9 \\ 3+4 \\ 14 \\ 1 \\ 2+6 \end{bmatrix} = \begin{bmatrix} 20 \\ 7 \\ 14 \\ 1 \\ 8 \end{bmatrix}.$$

Essa matriz coluna já é a transformação do nome do espião que, fazendo a conversão fica:

$$20 \to R,\ 7 \to A,\ 14 \to M\ 1 \to O,\ 8 \to N$$

Isto é, o espião se chama RAMON.

Ocorre que, embora essas atividades utilizem, de forma implícita, a Cifra de Hill, elas são construídas a partir de partes desse algoritmo de transformação de mensagens, com o objetivo de exercitar conteúdos específicos relacionados ao estudo de matrizes, sem a necessidade de aprofundamento em outros fundamentos matemáticos presentes nessa cifra. Na próxima seção, são apresentados os fundamentos matemáticos da Cifra de Hill, de modo a explicitar a articulação entre os diferentes conceitos envolvidos no processo de codificação e decodificação de mensagens.

2.2. Da mensagem à matriz: aspectos matemáticos da Cifra de Hill

A Cifra de Hill pode ser compreendida como um percurso que se inicia em uma mensagem escrita e culmina em sua representação matricial. Nesta seção, esse percurso é explorado por meio da codificação de uma mensagem, a partir da qual são discutidos os principais aspectos matemáticos que fundamentam esse método criptográfico. A opção por essa abordagem permitirá que os conceitos sejam introduzidos conforme se fazem necessários, favorecendo uma compreensão integrada do procedimento criptográfico.

2.2.1 Primeiro passo: definindo um referencial alfabético

Como foi possível perceber pelos exemplos 2.1.1 e 2.1.2, é preciso definir uma referência alfabética para usar em todo o processo. Essa escolha não será, necessariamente, o alfabeto da linguagem natural, no caso, o alfabeto da Língua Portuguesa, mas será um conjunto de caracteres cujo qual o remetente e o destinatário da mensagem conseguem construir ou entender mensagens a partir do agrupamento desses itens. Além disso, para cada caractere deve-se atribuir um valor numérico, isto é, dado um conjunto de n caracteres, deve-se atribuir ou um valor entre 0 e $n-1$ ou um valor entre 1 e n, na ordem que for preferível, mas garantindo que não haja repetição dos valores entre os itens.

Doravante, adota-se, a partir de agora, o conjunto de 27 caracteres abaixo, constituído pelos 26 itens do alfabeto da Língua Portuguesa e pelo hífen (-), que será usado para espaços ou para complementar mensagens. Nesse conjunto foi designado os valores de 0 a 26 seguindo a ordem do alfabeto comum e o último número sendo atribuído ao hífem.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	-
13	14	15	16	17	18	19	20	21	22	23	24	25	26

Como forma de exemplificação, a mensagem "CÓDIGO SECRETO" vira "CODIGO-SECRETO", isto é, a acentuação foi omitida e o espaço entre as palavras foi trocado pelo hífen. A partir disso, cada parte da mensagem é trocada pelo seu respectivo número da referência.

$$C \to 2\ O \to 14\ D \to 3\ I \to 8\ G \to 6\ O \to 14\ - \to 26\ S \to 18\ E \to 4\ C \to 2\ R \to 17\ E \to 4\ T \to 19\ O \to 14$$

2.2.2 Segundo passo: escolha da matriz-chave

Definido o referencial alfabético, o passo seguinte consiste na escolha da matriz-chave, elemento central da Cifra de Hill, responsável por transformar os blocos numéricos da mensagem

em novos blocos codificados. Para que os processos de codificação e decodificação sejam possíveis, essa matriz deve ser quadrada e invertível no conjunto dos inteiros módulo 27, ou seja, o resto da divisão do seu determinante por 27 tem que ser primo com 27, ou ainda, o mdc entre esses dois valores tem que ser 1.

O 27 não foi escolhido por acaso, é o valor associado ao referencial alfabético adotado na subseção anterior. Em termos práticos, o determinante da matriz-chave ser relativamente primo a 27 isso implica a existência de uma inversa capaz de decodificar a mensagem posteriormente.

Ocorre que, a ordem da matriz pode ser definida a critério do remetente da mensagem, no entanto, essa escolha resulta no tamanho dos blocos em que a mensagem será separada para codificação. Por ora, será utilizado para a exemplificação, a matriz C de ordem 2 abaixo.

$$C = \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix}$$

De fato, C é invertível para 27 caracteres, pois, seu determinante é:

$$\det C = 4 \cdot 10 - 2 \cdot 4 = 40 - 8 = 32$$

Mas ocorre que $32 = 1 \cdot 27 + 5$, ou seja, o resto da divisão de 32 por 27 é 5 ou, ainda, $32 \equiv 5 \ mod(27)$. Como 5 e 27 são primos entre si, já que o $mdc(5,27) = 1$, a matriz C é invertível para o alfabeto com 27 caracteres e pode ser usada para codificar mensagens a partir de agora.

2.2.3 Terceiro passo: codificando a mensagem

Definidos o alfabeto de referência e a representação numérica dos caracteres, inicia-se o processo de codificação propriamente dito. Nesta etapa, a mensagem é transformada por meio da multiplicação das matrizes colunas associados aos blocos de letras por a matriz-chave C previamente escolhida na seção anterior, conforme os princípios da Cifra de Hill. Esse procedimento permite articular, de forma concreta, conceitos de matrizes e operações matriciais, evidenciando o papel desses conteúdos na construção de um método criptográfico.

Já que a matriz-chave tem ordem 2, a mensagem escolhida "CODIGO-SECRETO"deve ser separada em blocos com dois caracteres que serão associados às entradas da matriz coluna que representará esse bloco. Assim, tem-se:

$$CO \rightarrow \begin{bmatrix} C \\ O \end{bmatrix} = \begin{bmatrix} 2 \\ 14 \end{bmatrix}$$

Multiplicando essa matriz pela matriz-chave:

$$\begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} 4 \cdot 2 + 2 \cdot 14 \\ 4 \cdot 2 + 10 \cdot 14 \end{bmatrix} = \begin{bmatrix} 8 + 28 \\ 8 + 140 \end{bmatrix} = \begin{bmatrix} 36 \\ 148 \end{bmatrix}$$

Só que 36 e 148 não são números que podem ser associados ao referencial alfabético, por isso, trabalha-se com os restos das suas divisões por 27, assim, mediante as igualdades $36 = 1 \cdot 27 + 9$ e $148 = 5 \cdot 27 + 13$, tem-se $36 \equiv 9 \ mod(27)$ e $148 \equiv 13 \ mod(27)$. Portanto,

$$CO \to \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} 36 \\ 148 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 13 \end{bmatrix} \ mod(27) \ \to JN$$

Analogamente, para os outros blocos de letras:

$$DI \to \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 8 \end{bmatrix} = \begin{bmatrix} 28 \\ 92 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 11 \end{bmatrix} \ mod(27) \ \to BL$$

$$GO \to \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 14 \end{bmatrix} = \begin{bmatrix} 52 \\ 164 \end{bmatrix} \equiv \begin{bmatrix} 25 \\ 2 \end{bmatrix} \ mod(27) \ \to ZC$$

$$-S \to \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \cdot \begin{bmatrix} 26 \\ 18 \end{bmatrix} = \begin{bmatrix} 140 \\ 284 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 14 \end{bmatrix} \ mod(27) \ \to FO$$

$$EC \to \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 2 \end{bmatrix} = \begin{bmatrix} 20 \\ 36 \end{bmatrix} \equiv \begin{bmatrix} 20 \\ 9 \end{bmatrix} \ mod(27) \ \to UJ$$

$$RE \to \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 76 \\ 108 \end{bmatrix} \equiv \begin{bmatrix} 22 \\ 0 \end{bmatrix} \ mod(27) \ \to WA$$

$$TO \to \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 14 \end{bmatrix} = \begin{bmatrix} 104 \\ 216 \end{bmatrix} \equiv \begin{bmatrix} 23 \\ 0 \end{bmatrix} \ mod(27) \ \to XA$$

Dessa forma, a mensagem "CODIGO-SECRETO" foi codificada para "JNBLZCFOUJWAXA".

2.2.4 A matemática por trás da decodificação

Após a realização do processo de codificação, surge a necessidade de recuperar a mensagem original a partir da informação criptografada. A decodificação, na Cifra de Hill, fundamenta-se na existência da matriz inversa da matriz-chave utilizada na codificação. Dessa forma, esta subseção tem como objetivo explicitar os fundamentos matemáticos que garantem a reversibilidade do processo, destacando o papel do determinante, da invertibilidade e das operações matriciais na reconstrução da mensagem original.

Iniciando pelo determinante da matriz-chave, ou melhor, pelo resto da divisão desse determinante por 27, deve-se encontrar um número entre 1 e 26 que, ao multiplicar por esse valor, dê um número cujo resto por 27 seja igual a 1. Esse número é chamado *inverso multiplicativo* e ele será fator fundamental para encontrar a matriz de decodificação.

Exemplo 2.2.1. *6 não é o inverso multiplicativo de C.*

De fato, $\det C = 32 \equiv 5 \ mod(27)$. Logo, $6 \cdot 5 = 30 \equiv 3 \ mod(27) \not\equiv 1 \ mod(27)$.

Exemplo 2.2.2. *11 é o inverso multiplicativo de C.*

Pela mesma ideia de que det $C = 32 \equiv 5\ mod(27)$, tem-se $11 \cdot 5 = 55 \equiv 1\ mod(27)$.

Agora, dispondo da informação de que o 11 é inverso multiplicativo de C, basta multiplicá-lo pela matriz adjunta de C, a $Adj(C)$, e o resultado será a matriz de decodificação D, capaz de recuperar a mensagem inicial.

$$C = \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix} \rightarrow Adj(C) = \begin{bmatrix} 10 & -2 \\ -4 & 4 \end{bmatrix}.$$

Assim,

$$D = 11 \cdot Adj(C) = 11 \cdot Adj(C) = \begin{bmatrix} 10 & -2 \\ -4 & 4 \end{bmatrix} = 11 \cdot \begin{bmatrix} 111 & -22 \\ -44 & 44 \end{bmatrix} \equiv \begin{bmatrix} 2 & 5 \\ 10 & 17 \end{bmatrix} mod(27).$$

Para entender por que $-22 \equiv 5 \mod(27)$, basta observar que $-22 = -1 \cdot 27 + 5$, assim, o resto da divisão de -22 por 27 é 5. Da mesma forma $-44 \equiv 10 \mod(27)$, pois $-44 = -2 \cdot 27 + 10$.

Determinada a matriz de decodificação, correspondente à inversa da matriz-chave no sistema modular considerado, procede-se à recuperação da mensagem original. Tal etapa baseia-se na propriedade de que a aplicação sucessiva de uma matriz e de sua inversa resulta na identidade, garantindo a reversibilidade do processo de codificação da Cifra de Hill. Para tanto, multiplica-se a matriz de decodificação por cada matriz coluna dos blocos de dois caracteres da mensagem codificada "JNBLZCFOUJWAXA", de forma similar ao processo de codificação.

$$JN \rightarrow \begin{bmatrix} 2 & 5 \\ 10 & 17 \end{bmatrix} \cdot \begin{bmatrix} 9 \\ 13 \end{bmatrix} = \begin{bmatrix} 83 \\ 311 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 14 \end{bmatrix} mod(27) \rightarrow CO$$

$$BL \rightarrow \begin{bmatrix} 2 & 5 \\ 10 & 17 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 11 \end{bmatrix} = \begin{bmatrix} 57 \\ 197 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 8 \end{bmatrix} mod(27) \rightarrow DI$$

$$ZC \rightarrow \begin{bmatrix} 2 & 5 \\ 10 & 17 \end{bmatrix} \cdot \begin{bmatrix} 25 \\ 2 \end{bmatrix} = \begin{bmatrix} 60 \\ 284 \end{bmatrix} \equiv \begin{bmatrix} 6 \\ 14 \end{bmatrix} mod(27) \rightarrow GO$$

$$FO \rightarrow \begin{bmatrix} 2 & 5 \\ 10 & 17 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} 80 \\ 288 \end{bmatrix} \equiv \begin{bmatrix} 26 \\ 18 \end{bmatrix} mod(27) \rightarrow -S$$

$$UJ \rightarrow \begin{bmatrix} 2 & 5 \\ 10 & 17 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 9 \end{bmatrix} = \begin{bmatrix} 85 \\ 353 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 2 \end{bmatrix} mod(27) \rightarrow EC$$

$$WA \rightarrow \begin{bmatrix} 2 & 5 \\ 10 & 17 \end{bmatrix} \cdot \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 44 \\ 220 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 4 \end{bmatrix} mod(27) \rightarrow RE$$

$$XA \rightarrow \begin{bmatrix} 2 & 5 \\ 10 & 17 \end{bmatrix} \cdot \begin{bmatrix} 23 \\ 0 \end{bmatrix} = \begin{bmatrix} 44 \\ 230 \end{bmatrix} \equiv \begin{bmatrix} 19 \\ 14 \end{bmatrix} \ mod(27) \ \rightarrow TO$$

Desse modo, "JNBLZCFOUJWAXA"retornou a "CODIGO-SECRETO".

Ao longo deste capítulo, buscou-se articular a análise do livro didático adotado no Ensino Médio com a apresentação dos fundamentos matemáticos da Cifra de Hill, evidenciando como conteúdos tradicionalmente abordados de forma fragmentada podem ser integrados em uma proposta contextualizada e significativa. A partir da codificação e decodificação de uma mensagem, foi possível explorar conceitos como matrizes, determinantes, invertibilidade e aritmética modular, ressaltando suas aplicações em um contexto criptográfico acessível ao nível do Ensino Médio.

Essa abordagem evidencia o potencial da Cifra de Hill como recurso pedagógico para o ensino desses conteúdos, ao promover uma aprendizagem que vai além do caráter procedimental, favorecendo a compreensão conceitual e o engajamento dos estudantes. Nesse sentido, os fundamentos matemáticos aqui discutidos constituem a base teórica necessária para a implementação do produto educacional proposto, cuja concepção e organização serão detalhadas no capítulo seguinte.

3. CONCEPÇÃO DO PRODUTO EDUCACIONAL "CIFRANDO MATRIZES E DECIFRANDO SEGREDOS"

Propostas educacionais que favorecem a exploração de conceitos matemáticos de forma dinâmica e interativa têm se mostrado grandes aliadas no processo de ensino e aprendizagem, especialmente quando alinhadas ao uso de tecnologias digitais.

Entre essas tecnologias, as planilhas digitais têm destaque a visualização de dados, a automatização de cálculos e a experimentação de diferentes situações, sem substituir a compreensão conceitual. Nesse sentido, o Excel apresenta-se como uma ferramenta acessível e familiar a muitos estudantes e professores, configurando-se como um recurso potencial para o desenvolvimento de atividades envolvendo matrizes e operações matriciais, como as propostas neste trabalho. Em conformidade com Oliveira (2021), quando diz que o uso do Excel no contexto educacional tem se mostrado um tema amplo e passível de diversas reflexões, especialmente no ensino de Matemática, uma vez que essa ferramenta contribui para o enriquecimento dos conhecimentos ao favorecer a exploração de conteúdos em sala de aula.

Dessa forma, o produto educacional desenvolvido consiste em quatro planilhas que automatizam o processo de utilização da Cifra de Hill sem perder o caráter funcional e matemático, permitindo que os estudantes concentrem sua atenção na compreensão dos conceitos envolvidos, e não apenas na execução de cálculos. Além dessas, foi construída mais uma planilha, com caráter de auxílio para a solução de sistemas de congruências modulares, esta foi contemplada no capítulo *V* do manual do produto educacional.

Este capítulo tem a pretensão de apresentar as etapas da concepção das planilhas, sem entrar em detalhes sobre a sua utilização. No entanto, no apêndice deste trabalho encontra-se o manual *Cifrando Matrizes e Decifrando Segredos*, constituído como parte fundamental do Produto Educacional construído.

3.1. Concepção da planilha da matriz-chave

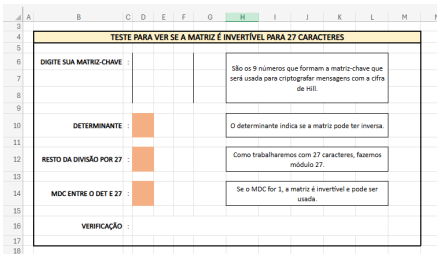
Para a construção das planilhas foi utilizado o Excel Online, através do pacote da Microsoft 365. Cada planilha exerce papel fundamental da estrutura da cifra de Hill e foram feitas em duas versões, uma para a matriz-chave de ordem 2 e uma para a matriz-chave de ordem 3. A fim de condensar as informações, aqui será apresentada a construção das planilhas de ordem 3, sendo a de ordem 2 construída de forma análoga.

A primeira das planilhas verifica se a matriz que deseja-se usar é realmente invertível para o módulo 27. Portanto, foi construída a interface da Figura 3.1, e foi adotado, nas células em laranja, as seguintes funções:

(i) $D10 \rightarrow = MATRIZ.DETERM(D6:F8)$

(ii) $D12 \rightarrow = MOD(D10;27)$

Figura 3.1 A base da primeira planilha.



(iii) $D14 \rightarrow = MDC(D12;27)$

O Excel já dispõe das funções necessárias para cada cálculo, sendo elas, a (i) responsável por calcular o determinante da matriz de ordem 3 informada, a (ii) com o objetivo de aplicar o módulo 27 (encontrar o resto da divisão por 27) ao valor do determinante encontrado e a (iii) é designada para calcular o MDC entre a (ii) e 27. Veja na Figura 3.2 esse processo na prática, após serem informadas as entradas numéricas da possível matriz-chave.

Figura 3.2 Primeira planilha após a inserção das funções.

3												
4		TESTE PARA VER SE A MATRIZ É INVERTÍVEL PARA 27 CARACTERES										
5												
6		DIGITE SUA MATRIZ-CHAVE :	1	2	3		São os 9 números que formam a matriz-chave que será usada para criptografar mensagens com a cifra de Hill.					
7			3	2	1							
8			1	4	1							
9												
10		DETERMINANTE :	24				O determinante indica se a matriz pode ter inversa.					
11												
12		RESTO DA DIVISÃO POR 27 :	24				Como trabalharemos com 27 caracteres, fazemos módulo 27.					
13												
14		MDC ENTRE O DET E 27 :	3				Se o MDC for 1, a matriz é invertível e pode ser usada.					
15												
16		VERIFICAÇÃO :										
17												
18												

Para a parte de verificação, utiliza-se a seguinte fórmula

$$= SE(D14 = 1;"Sim,\ a\ matriz\ \ invertvel\ para\ 27\ caracteres";\\ "Nao,\ a\ matriz\ no\ \ invertvel\ para\ 27\ caracteres")$$

E, ainda, para efeitos estéticos, cria-se duas regras indo em "Formatação Condicional"→ "Nova Regra"→ Formatar Células em que uma função é "verdadeira". As regras devem ficar como estão na Figura 3.3.

Assim, se for inserida uma matriz invertível módulo 27 algumas partes da planilha ficarão verdes e, caso contrário, essas mesmas partes irão ficar vermelhas, como exposto nas Figuras 3.4 e 3.5.

Figura 3.3 Formatações condicionais usadas.

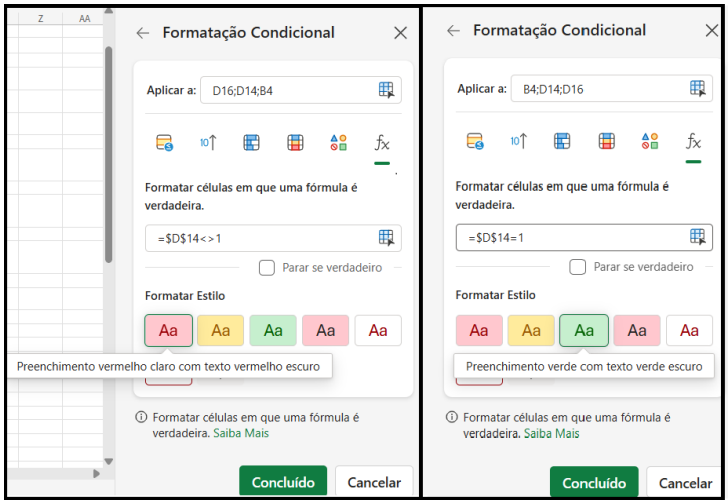


Figura 3.4 Primeira planilha com uma matriz não invertível em módulo 27.

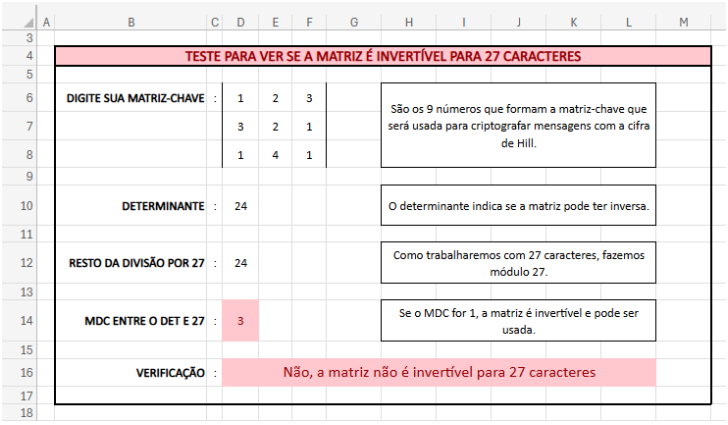
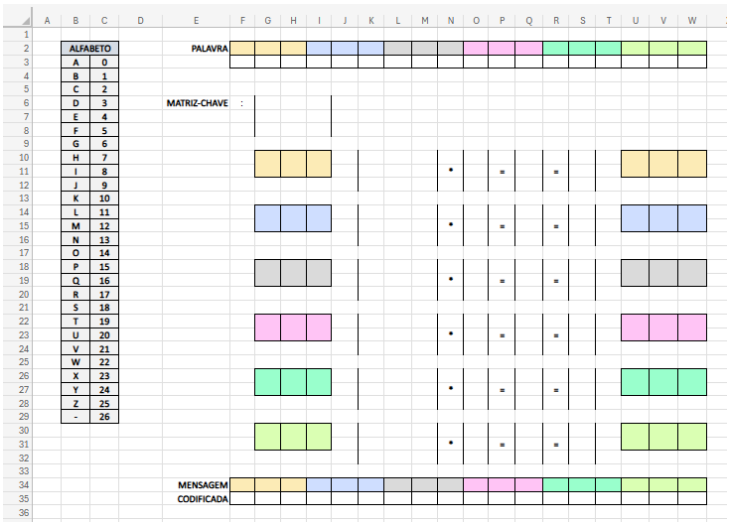


Figura 3.5 Primeira planilha com uma matriz invertível em módulo 27.

3.2. Desenvolvimento da planilha de codificação

A segunda planilha, ou planilha de codificação tem por base a interface da Figura 3.6.

Figura 3.6 Base da segunda planilha.

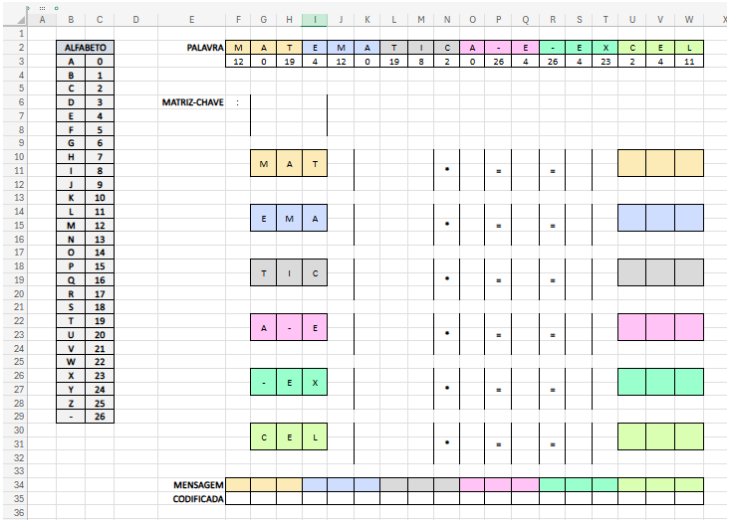


As células coloridas da segunda linha da tabela constituem os espaços para serem colocados os caracteres da mensagem que será codificada, dessa forma, pode ter até 18 caracteres. Em cada célula abaixo das coloridas da linha 2, será utilizada a fórmula PROCV, para, de forma automática, procurar o referencial numérico no alfabeto.

Exemplo 3.2.1. *Na célula F3 foi usada a fórmula "*$= PROCV(F2;\$B\$3:\$C\$29;2;FALSO)$*", na G3 a fórmula "*$= PROCV(G2;\$B\$3:\$C\$29;2;FALSO)$*"e assim em diante, até a célula W3.*

Além disso, no meio da planilha, no ambiente de transformação da mensagem, será utilizado o "="para igualar células e transportar os trios de caracteres da mensagem para esse ambiente. A figura 3.7 exemplifica as mudanças com a mensagem "MATEMATICA-E-EXCEL".

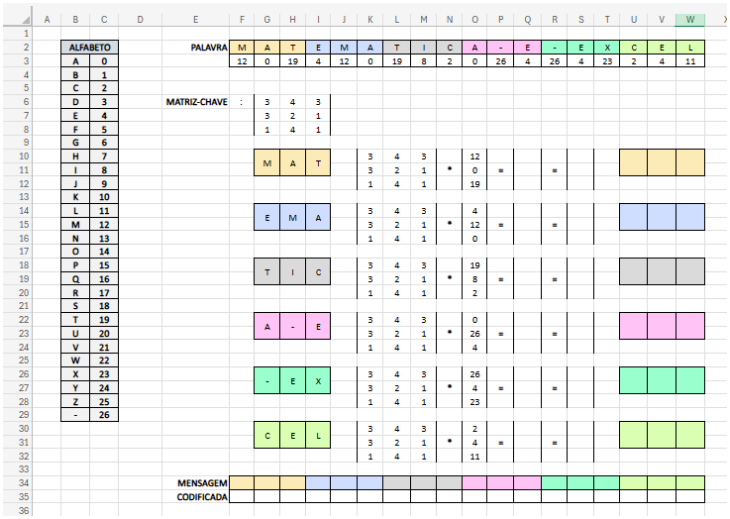
Figura 3.7 Planilha de codificação com a mensagem inicial inserida.



Além disso, foram igualadas as células de cada matriz de ordem 3 do ambiente de transformação da mensagem à respectiva célula da matriz-chave e, também, cada célula das matrizes

coluna à referência numérica do caractere da mensagem, como mostrado na Figura 3.8.

Figura 3.8 Inserção da matriz-chave e das matrizes coluna de cada trecho da mensagem.

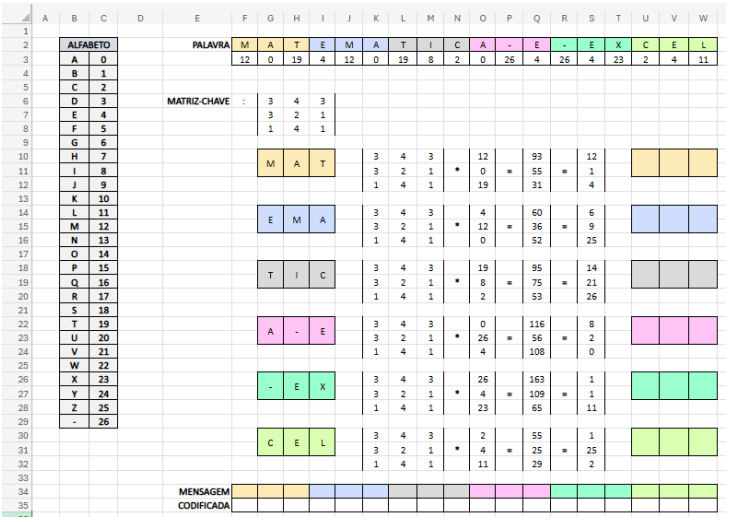


Para as multiplicações de matrizes no ambiente de transformação da mensagem foi utilizada a fórmula MATRIZES.MULT, selecionando as células de cada matriz que se desejava fazer a multiplicação. Logo depois, na coluna S foi aplicada a fórmula MOD, para encontrar os módulos das entradas das matrizes resultantes das multiplicações. Essas adições geraram o exposto na Figura 3.9.

Exemplo 3.2.2. *Na célula* $O10$ *foi inserido "*$= MATRIZ.MULT(K10:M12;O10:O12)$*".*

Exemplo 3.2.3. *Na célula* $S10$ *foi inserido "*$= MOD(Q10;27)$*".*

Figura 3.9 Multiplicação das matrizes.

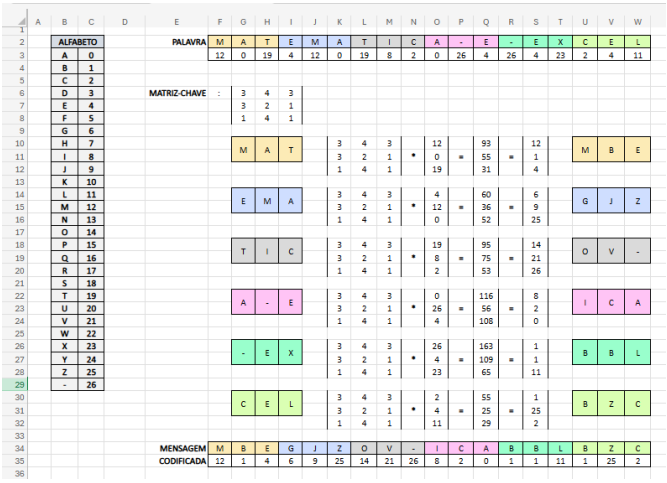


Para finalizar esta planilha bastou transformar cada número das últimas matrizes coluna em seu respectivo caractere do alfabeto, para tanto, foram usadas as fórmulas INDICE E CORRESP juntas, como no exemplo abaixo.

Exemplo 3.2.4. *U*10 *recebeu o comando* = *INDICE*($*B*$3 : $*B*$29;*CORRESP*(*S*10;$*C*$3 : $*C*$29;0)), *V*10 *recebeu a fórmula* = *INDICE*(*B*3 :*B*29;*CORRESP*(*S*11;$*C*$3 : $*C*$29;0)) *e W*10 *recebeu* = *INDICE*(*B*3 :*B*29;*CORRESP*(*S*12;$*C*$3 : $*C*$29;0)).

Além disso, voltou-se a utilizar = para transferir cada pedaço da mensagem criptografada para a parte final da planilha. Observa-se o resultado final desta planilha na Figura 3.10.

Figura 3.10 Planilha de codificação finalizada.

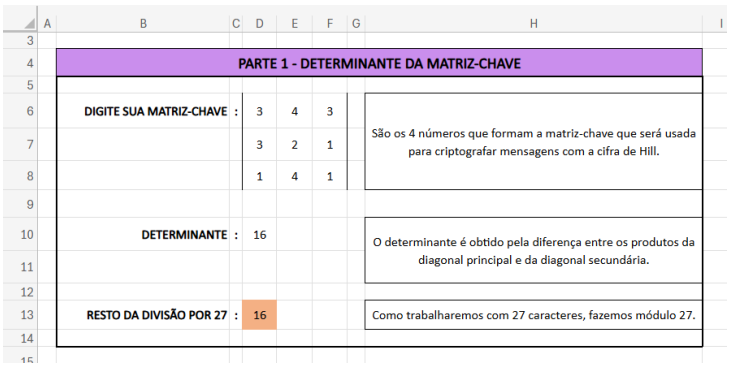


3.3. Construção da planilha da matriz de decodificação

A planilha eletrônica que dá suporte na descoberta da matriz de decodificação é a maior das planilhas, pois é constituída de 3 partes, a primeira para obtenção do determinante da matriz-chave, a segunda para o inverso multiplicativo desse determinante e, enfim, a terceira parte para a obtenção final da matriz que irá transformar os códigos "confusos"na mensagem original.

A primeira parte desta planilha (Figura 3.11) é semelhante ao exposto na primeira planilha, exceto pela omissão do MDC e da verificação, pois são informações desnecessárias ao processo atual.

Figura 3.11 Parte I - Determinante da matriz- chave.



Já a segunda parte (Figura 3.12), que tem por objetivo detalhar o processo de encontrar o inverso multiplicativo do determinante da matriz-chave, utiliza-se das mesmas fórmulas já mencionadas nas construções, mas com um novo olhar.

Na linha cinco foram expostas todas as possibilidades para o inverso multiplicativo sem que houvesse repetição e sem que gerasse a possibilidade de um determinante de matriz inversível módulo 27 ficasse sem inverso multiplicativo, isto é, foram atribuídos os números de 1 a 26. Em cada linha abaixo desta foi utilizada uma mesma fórmula na maioria das células, respeitando-se a ordem de cada número, são elas:

Linha 6. A multiplicação da célula $K6$ pela respectiva célula da linha 5.

Exemplo 3.3.1. *Para a L6 foi atribuído "*$= \$K\$6 * L5$*".*

Linha 7. O resto da divisão da respectiva célula da linha 6 por 27.

Exemplo 3.3.2. *Para a L7 foi atribuído "*$= MOD(L6;27)$*".*

Figura 3.12 Parte II - Inverso multiplicativo do determinante da matriz- chave.

	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK
3																												
4			PARTE 2 - O INVERSO MULTIPLICATIVO																									
5			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
6	MULTIPLICADO POR	16	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240	256	272	288	304	320	336	352	368	384	400	416
7	RESTO POR	27	16	5	21	10	26	15	4	20	9	25	14	3	19	8	24	13	2	18	7	23	12	1	17	6	22	11
8																												
9		TEM ALGUM NÚMERO DE 1 A 26 CUJO, DEPOIS DA MULTIPLICAÇÃO, O RESULTADO DE SEU RESTO POR 27 DEU 1?																										
10		SIM	Esse número é o **inverso multiplicativo do determinante** da Matriz-chave e será usado para a **parte 3**.																									
11			**Obs.:** Coloque ele no quadrado verde da **Parte 3**.																									
12		NÃO	A matriz informada não pode ser matriz-chave para a Cifra de Hill com 27 caracteres. Volte para a primeira planilha e verifique que ela não é invertível.																									
13																												
14																												

A terceira e última parte desta planilha (Figura 3.13) é constituída pela construção da inversa da matriz de ordem 3. Para isso, foi exposto primeiramente a matriz de cofatores da matriz-chave, em sequência, a matriz adjunta dela e, por fim, sua inversa módulo 27.

A matriz de cofatores foi formulada manualmente, pois não há função pronta no Excel para que os cálculos sejam feitos automaticamente, assim, foram usadas as fórmulas:

$$\text{(I)}\ \ D20 \rightarrow "= MATRIZ.DETERM(E7:F8)"$$

$$\text{(II)}\ \ E20 \rightarrow "= -(D7 * F8 - F7 * D8)"$$

$$\text{(III)}\ \ F20 \rightarrow "= MATRIZ.DETERM(D7:E8)"$$

$$\text{(IV)}\ \ D21 \rightarrow "= -(E6 * F8 - F6 * E8)"$$

(V) $E21 \rightarrow$ "$= D6 * F8 - F6 * D8$"

(VI) $F21 \rightarrow$ "$= -(D6 * E8 - E6 * D8)$"

(VII) $D22 \rightarrow$ "$= MATRIZ.DETERM(E6 : F7)$"

(VIII) $E22 \rightarrow$ "$= -(D6 * F7 - F6 * D7)$"

(IX) $F22 \rightarrow$ "$= MATRIZ.DETERM(D6 : E7)$"

Figura 3.13 Parte II - Inverso multiplicativo do determinante da matriz- chave.

PARTE 3 - A MATRIZ DE DECODIFICAÇÃO					
MATRIZ DE COFATORES DA MATRIZ-CHAVE	:	-2	-2	10	A matriz de cofatores de uma matriz de ordem 3 é formada pelos cofatores de cada elemento, obtidos a partir dos determinantes das submatrizes correspondentes, considerando os sinais associados às suas posições.
		8	0	-8	
		-2	6	-6	
ADJUNTA DA MATRIZ-CHAVE		-2	8	-2	É a transposta da Matriz de cofatores da Matriz-chave.
		-2	0	6	
		10	-8	-6	
INVERSO MULTIPLICATIVO DA MATRIZ-CHAVE	:	22			Deve ser obtido na tabela da Parte 2.
MULTIPLICAÇÃO	:	-44	176	-44	É a Matriz Adjunta multiplicada pelo Inverso Multiplicativo do determinante da Matriz-chave.
		-44	0	132	
		220	-176	-132	
MATRIZ DE DECODIFICAÇÃO	:	10	14	10	É a Matriz Inversa considerando-se os restos da divisão de suas entradas por 27.
		10	0	24	
		4	13	3	

As demais matrizes desta parte foram obtidas com funções já utilizadas antes, seguindo a descrição apresentada na própria tabela (Figura 3.13).

Ressalta-se que a organização das planilhas foi pensada de modo a tornar explícitas as etapas matemáticas envolvidas no processo, permitindo ao professor acompanhar e discutir com os estudantes cada fase da construção da matriz inversa, sem a necessidade de aprofundamento em aspectos técnicos do software.

De forma geral, o conjunto de planilhas foi concebido para atuar como um suporte pedagógico ao ensino da Cifra de Hill, favorecendo a visualização das operações com matrizes e a

compreensão da relação entre determinante, cofatores e invertibilidade. Assim, o uso do Excel não substitui o raciocínio matemático, mas atua como uma ferramenta que auxilia na exploração dos conceitos, possibilitando maior foco na interpretação dos resultados e na discussão conceitual.

Os procedimentos operacionais detalhados para a utilização das planilhas, bem como orientações didáticas e sugestões de encaminhamento em sala de aula, encontram-se descritos no manual do professor, apresentado como parte integrante do produto educacional no apêndice desta dissertação.

CONSIDERAÇÕES FINAIS

No decorrer deste trabalho, investigou-se o uso da Cifra de Hill como recurso didático para o ensino de Matrizes e Determinantes no Ensino Médio, articulando fundamentos matemáticos da criptografia clássica ao uso de planilhas eletrônicas, em especial o software Excel. A proposta desenvolvida buscou integrar conteúdos tradicionalmente abordados de forma abstrata a uma aplicação contextualizada, aproximando a Matemática de situações significativas e relacionadas ao universo tecnológico vivenciado pelos estudantes.

Para tanto, foram apresentados alguns aspectos históricos da criptografia, evidenciando sua relevância social desde a Antiguidade até a atualidade, bem como os fundamentos matemáticos que sustentam a Cifra de Hill. A abordagem adotada privilegiou uma construção progressiva desses conceitos, aplicados à construção da ideia presente na Cifra de Hill, respeitando o nível de complexidade adequado ao Ensino Médio e buscando subsidiar a prática docente.

Como desdobramento do estudo teórico, foi concebido o produto educacional Cifrando Matrizes e Decifrando Segredos, constituído por um conjunto de planilhas eletrônicas que automatizam os processos de codificação e decodificação da Cifra de Hill, sem descaracterizar o raciocínio matemático envolvido. A utilização do Excel mostrou-se um recurso potencial para favorecer a visualização do estudo matricial, permitindo que estudantes e professores concentrem sua atenção na compreensão conceitual dos procedimentos, e não apenas na execução mecânica dos cálculos.

As planilhas desenvolvidas foram organizadas de modo a tornar explícitas as etapas matemáticas do algoritmo criptográfico, possibilitando ao professor explorar, discutir e problematizar cada fase do processo em sala de aula. Nesse sentido, o recurso tecnológico não se apresenta como substituto da Matemática, mas como um mediador que amplia as possibilidades de experimentação, análise e interpretação dos resultados.

Em linhas gerais, compreende-se que a proposta apresentada contribui para o ensino de Matrizes ao articular Matemática, tecnologia e criptografia em uma abordagem contextualizada e significativa. Espera-se que este trabalho possa incentivar professores a explorarem metodologias semelhantes, utilizando recursos digitais acessíveis como aliados no processo de ensino e aprendizagem, bem como fomentar novas investigações sobre o uso da criptografia e de tecnologias digitais na Educação Matemática.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Luana Macêdo Cavalcante Chacon de. **Uma revisão sobre os tipos de criptografia e sua aplicação na proteção de dados em trânsito**. Dissertação de Mestrado, Universidade Federal da Paraíba (UFPB), 2025.

ANDRADE, Luciana Vieira. **Saberes docentes e conhecimento didático do professor mobilizados na escolha do livro didático de matemática**. Dissertação de Mestrado, Universidade Estadual Paulista (UNESP), 2024.

ARAUJO, Cláudia Lima de; SANTOS, Queila Pereira; RIBEIRO, Hellen Maura Lucidia; FREITAS, Eliene Barbosa do Nascimento de; COUTINHO Diógenes José Gusmão. **Evasão escolar: causas e impacto da evasão escolar no brasil e no mundo**. Revista Ibero-Americana de Humanidades, Ciências e Educação- REASE, 11(1), 2025.

ARAVÉCHIA, Lucas Sgarbi; DIAN, Mauricio de Oliveira. **Criptografia RSA: sua importância e utilização em sistemas atuais**. Interface Tecnológica, 21(1), 2024.

BONJORNO, José Roberto; JÚNIOR, José Ruy Giovanni; SOUSA, Paulo Roberto Câmara de. Prisma matemática: sistemas, matemática financeira e grandezas, volume 13. Editora FTD, 2020.

BRANDÃO, Mariana Martíns Duraes. **Uma adaptação da cifra de hill para estudo de matrizes**. Dissertação de Mestrado, Universidade Federal de Ouro Preto (UFOP), 2017.

CAVALCANTE, André L.B. **Teoria dos números e criptografia**. Faculdades Integradas (UPIS)-Faculdade de Tecnologia, 2009.

FERREIRA, Jordão Tavares; SANTOS, Claudiene dos. **O uso da tecnologia digital em sala de aula: reflexos no ensino de matemática**. Revista Brasileira de Ensino e Aprendizagem (REBENA), 13, 2025.

GROENWALD, Claudia Lisete Oliveira; ITANK, Rosvita Fuelber. **Currículo de matemática e o tema criptografia no ensino médio**. EDUCAÇÃO MATEMÁTICA EM REVISTA (RS), 1(8), 2007.

KRANZ, Bárbara Elisa; OLGIN, Clarissa de Assis. **Uma sequência didática com a temática criptografia para o ensino de matrizes do ensino médio**. 6º Fórum Nacional sobre Currículos de Matemática, 2024.

LAJOLO, Marisa. **Livro didático: um (quase) manual de usuário**. Revista Em Aberto, (69), 1996.

LIMA, Marta Gomes; ROCHA, Adriano Aparecido Soares da. **As tecnologias digitais no ensino de matemática**. Revista Ibero-Americana de Humanidades, Ciências e Educação - REASE, 8(5), 2022.

MARTÍNS, Wellington de Sousa. **Aplicação da álgebra moderna nos fundamentos da criptografia-cifras de César e cifras de Hill**. Dissertação de Mestrado, Universidade Federal do Tocantins (UFT), 2023.

MONFRE, G. A.; SILVA, F. G.; VICENTIN, A. C. **Criptografia na sociedade digital: Evolução, aplicações e desafios na proteção da informação**. Revista Matiz Online, 2023.

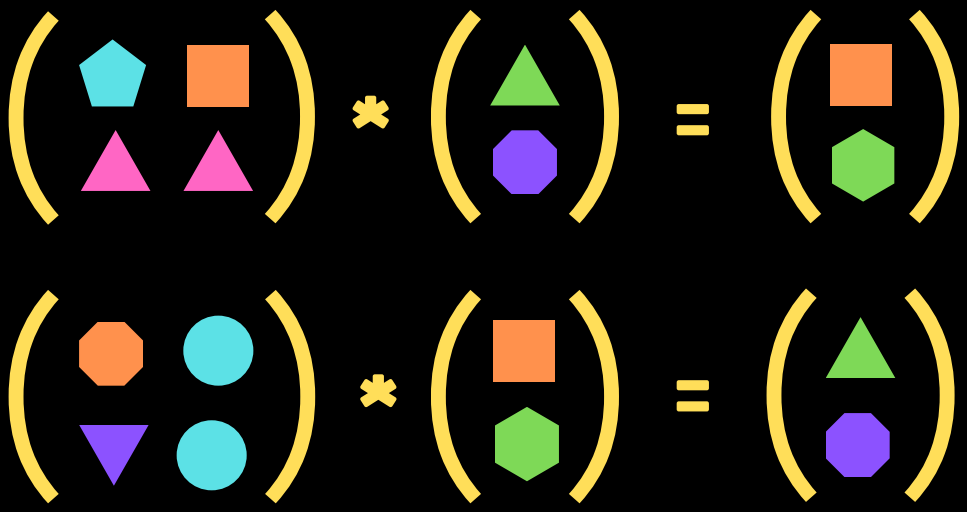
OLIVEIRA, Fabricio de Figueredo. **Excel: o uso das novas tecnologias no processo ensino-aprendizagem de matemática na educação básica**. Dissertação de Mestrado, Universidade Federal Rural do Semi Árido (UFERSA), 2021.

SILVA, Wellyngton Chaves Monteiro da. **Uma análise do programa escola 10 como política pública educacional para o estado de Alagoas**. Tese de Doutorado, Universidade Federal do Rio Grande do Sul (UFRGS), 2021.

SINGH, Simons. **O Livro dos Códigos**. Record, 14º edition, 2022.

MANUAL SOBRE A UTILIZAÇÃO DO EXCEL ALINHADO AOS FUNDAMENTOS MATEMÁTICOS DA CIFRA DE HILL PARA PROFESSORES DE MATEMÁTICA DO ENSINO MÉDIO

CIFRANDO MATRIZES E DECIFRANDO SEGREDOS



ANA CAROLINA GONÇALVES ARAÚJO
ISAAC ISNALDO BARBOSA

UNIVERSIDADE FEDERAL DE ALAGOAS

PROFMAT Mestrado Profissional em Matemática

Instituto de Matemática

MANUAL SOBRE A UTILIZAÇÃO DO EXCEL ALINHADO AOS FUNDAMENTOS MATEMÁTICOS DA CIFRA DE HILL PARA PROFESSORES DE MATEMÁTICA DO ENSINO MÉDIO

CIFRANDO MATRIZES
E DECIFRANDO SEGREDOS

ANA CAROLINA GONÇALVES ARAÚJO
ISAAC ISNALDO BARBOSA

UNIVERSIDADE FEDERAL DE ALAGOAS
PROFMAT Mestrado Profissional em Matemática
Instituto de Matemática

AO MEU PRIMEIRO
PROFESSOR DE
MATEMÁTICA, MARCELO
ARAÚJO, MEU PAI.
POR DESPERTAR EM MIM O
AMOR PELOS NÚMEROS E
ME ENSINAR O VALOR DA
PERSEVERANÇA.

CARTA AO PROFESSOR

É com grande satisfação e entusiasmo que apresento o produto educacional "Cifrando Matrizes e Decifrando Segredos", resultado de uma jornada de estudo e dedicação ao Mestrado Profissional em Matemática em Rede Nacional - PROFMAT.

O mundo está repleto de segredos matemáticos, e um dos mais fascinantes é a Criptografia. Muitas vezes, conceitos como Matrizes, Determinantes e Aritmética Modular parecem distantes da realidade, restritos aos livros didáticos. Minha maior motivação ao criar esta ferramenta e este manual foi justamente quebrar essa barreira!

Professor(a), o que você tem em mãos é mais do que uma simples planilha: é um laboratório interativo que transforma a complexidade da Cifra de Hill em uma missão de codificação e decodificação acessível e envolvente. Você verá, na prática, como o rigor da Álgebra Linear e a beleza da Matemática Pura e Aplicada se unem para proteger informações.

Este manual é seu guia nessa missão. Convido você a mergulhar, sem medo, no universo dos códigos secretos. Prepare-se para cifrar e, acima de tudo, para comprovar o poder da Matemática.

Ana Carolina

Professora de Matemática

CONTATOS

E-mail institucional: ana.goncalves@im.ufal.br

E-mail pessoal: carolinaaraujo.2573@gmail.com

Instagram: @carolinaa.aaraujo

Lattes: http://lattes.cnpq.br/3438501650845145

SUMÁRIO

Introdução

Bem-vindo ao Mundo da Cifra de Hill

"Ninguém deveria sentir orgulho por não saber matemática. O caminho para tirar essa aura impenetrável é não matar a curiosidade, é permitir que as pessoas explorem e brinquem com a matemática, especialmente desde jovens"
- Artur Avila

"Ninguém deveria sentir orgulho por não saber matemática", essa foi a reflexão feita em 2024 durante uma entrevista ao jornal Folha de São Paulo pelo pesquisador brasileiro Artur Ávila, primeiro latino-americano a ganhar a Medalha Fields.

Essa reflexão deve ecoar no coração e mente de qualquer professor(a) de matemática apaixonado(a) pelo que ensina e comprometido(a) com sua função. Em essência, o(a) educador(a) matemático(a) é um(a) matemático(a) que, transpassado seu amor ao trabalho matemático, resolveu ensinar.

> O fato é que a curiosidade existe. Eu a constato diariamente. A matemática dá medo, mas fascina ainda mais. Não é amada, mas todo mundo gostaria de amá-la. Ou pelo menos ser capaz de dar uma olhada indiscreta em seus tenebrosos mistérios. As pessoas tendem a achar que eles são inacessíveis, o que não é verdade. É perfeitamente aceitável gostar de música sem ser músico ou compartilhar uma bela refeição sem ser um grande cozinheiro. Por que, então, seria necessário ser matemático ou ter uma inteligência excepcional para entrar no mundo da matemática ou deixar a mente ser provocada pela álgebra ou pela geometria? Não é necessário entrar nos detalhes técnicos para entender as grandes ideias e se maravilhar com elas (Launay, 2019).

É com esse espírito de renovação e o objetivo de resgatar o prazer em estudar matemática que apresentamos o produto educacional "Cifrando Matrizes e Decifrando Segredos".

Ao utilizar a Cifra de Hill, este manual e a planilha interativa que o acompanha transformam a Álgebra Linear em uma atividade de espionagem, onde Matrizes, Determinantes e a Invertibilidade Modular (módulo 27) são as ferramentas essenciais para criar e desvendar códigos secretos, como também vivenciam o poder da Matemática na segurança da informação.

Parte 1 - A Cifra de Hill: História e Fundamentos

O ser humano sempre buscou formas de comunicação e, posteriormente, formas de proteger informações vitais. Da escrita hieroglífica à comunicação segura em transações bancárias, a necessidade de sigilo da informação deu origem à Criptografia, a arte e ciência de escrever em códigos. A própria palavra tem origem no grego “Kryptós”, que em português é o mesmo que “secreto”. “Para a criptografia isso seria escrever uma mensagem ou código de uma maneira na qual o receptor e remetente são os únicos capazes de decifrá-la.” (Costa, 2022).

É com o propósito de aplicar a Matemática de forma lúdica e funcional que este produto utiliza a Cifra de Hill como seu pilar pedagógico. Desenvolvida em 1929 pelo matemático americano Lester S. Hill, essa cifra é considerada um marco na história da criptografia por ter sido o primeiro sistema polialfabético a ser prático para o uso.

> No início do século XX, iniciam-se as primeiras tentativas de mecanização das técnicas criptográficas, pois os sistemas existentes, mono e polialfabéticos, estavam vulneráveis à análise de frequências. Uma das alternativas apresentadas consistia em agrupar as letras do texto normal, formando blocos com um número n de caracteres e, a cada conjunto formado, substituí-las por um conjunto n de letras cifradas. Esta técnica clássica de substituição, utilizando conceitos da Álgebra Linear e da Aritmética Modular, aprimorada por Lester S. Hill em 1929, deu origem ao que se denomina a Cifra de Hill (Jeanrenaud, 2013).

A grande inovação de Hill foi empregar a Álgebra Linear no processo de cifragem, transformando blocos de letras da mensagem em vetores e multiplicando-os por uma matriz-chave,

> “Nas cifras polialfabéticas, uma mesma letra na mensagem original pode ser substituída por letras diferentes o que dificulta o processo de decifração por análise de frequência, embora possa ser criptoanalisada por recursos de álgebra linear.” (Martíns, 2023).

Para que a decodificação seja possível, essa matriz precisa satisfazer uma condição matemática rigorosa: ser invertível dentro de um sistema de aritmética modular (no nosso caso, módulo 27). Este manual guiará o leitor passo a passo na compreensão e aplicação desses conceitos.

Parte 2 - O produto educacional: Acesso às planilha do Excel

Para prosseguir com o manual é preciso ter acesso às planilhas que serão explicadas ao decorrer dos capítulos a seguir. É possível acessá-las através dos QR Codes abaixo.

Google Drive
Pasta com as duas versões da planilha
https://acesse.one/OfEY4

Excel Online
Planilhas - ordem 2

Excel Online
Planilhas - ordem 3

Recomenda-se fazer uma cópia da planilha cujas matrizes estão na 2º ordem, para acompanhar este manual. As planilhas na 3º ordem são utilizadas de forma semelhante.

Capítulo I

A Chave

Sua Matriz Está Pronta para Criptografar?

"A educação é a chave para libertar o mundo e uma das maiores necessidades da humanidade." - Malba Tahan

Capítulo I
A Chave

Antes de começar a escrever mensagens secretas, é preciso garantir que você tem a ferramenta certa em mãos: uma matriz que funcione como uma chave confiável. Mas atenção! Nem toda matriz está apta para a missão.

Neste capítulo, vamos testar se a sua matriz quadrada de ordem 2 tem o que é necessário para entrar no mundo da criptografia com a Cifra de Hill, usando um alfabeto de 27 caracteres (de A a Z, mais o espaço). A etapa é simples, mas essencial: verificar se sua matriz é invertível no módulo 27, só assim ela poderá ser usada para codificar e decodificar mensagens secretas.

Você descobrirá como calcular o determinante, aplicar o módulo 27, e verificar se a matriz passa no teste de segurança. Pense nisso como o "scan de segurança" antes de liberar acesso ao cofre da informação.

PREPARE SUA MATRIZ, SIGA OS PASSOS E DESCUBRA:
ELA É SEGURA O BASTANTE PARA PROTEGER SEGREDOS?

1.1 Conhecendo a Primeira Planilha: Matriz-chave

Este módulo da planilha tem como propósito auxiliar os alunos a compreenderem como verificar se uma matriz de ordem 2 pode ser utilizada na Cifra de Hill, utilizando o alfabeto com 27 caracteres. Observe na imagem abaixo a interface criada com esse propósito, você pode ter acesso a ela através do link já disponibilizado na Parte 2 da introdução desse manual.

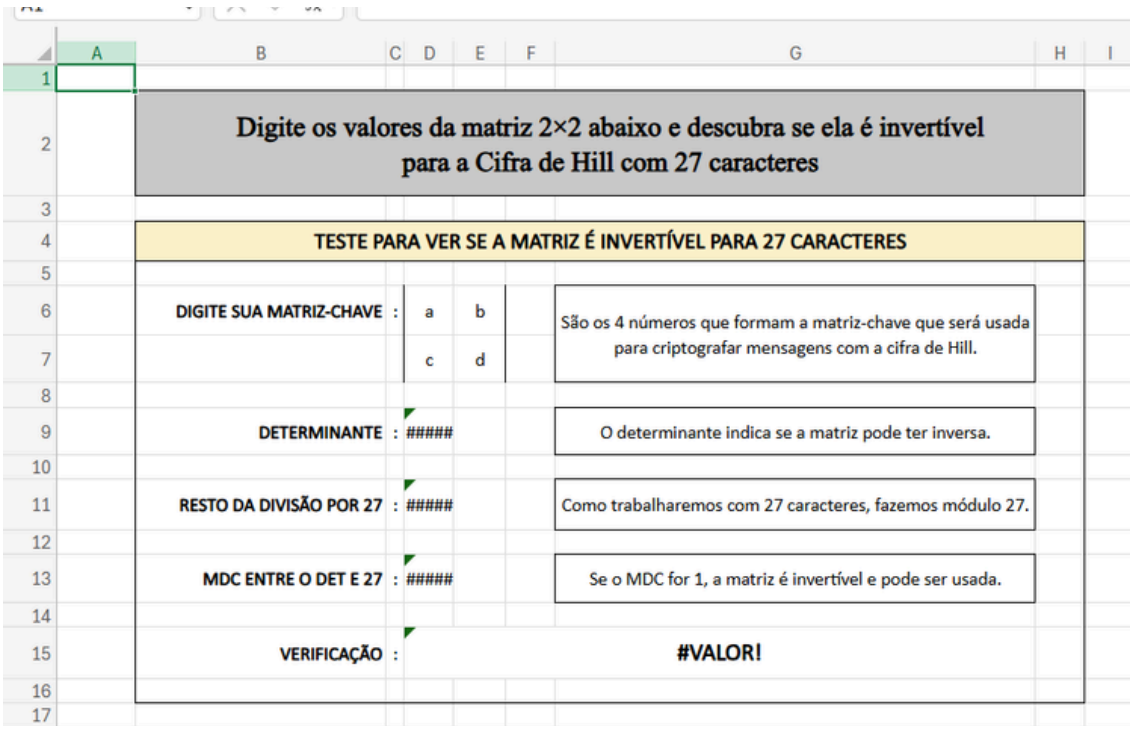


Imagem 1.1. interface da planilha “Matriz-chave”.

Nesta planilha, apenas as células D6, D7, E6 e E7 são editáveis. Essas células representam as entradas da matriz quadrada de ordem 2 que será utilizada como matriz de codificação na próxima etapa. Inicialmente, essas células contêm letras como marcadores de posição. O usuário deve substituí-las exclusivamente por valores numéricos.

Para garantir a integridade dos dados, as demais células da planilha estão protegidas contra edição. Além disso, a tabela está automatizada, para representar bem a validação ou não da utilização da matriz escrita.

Veja a seguir o que ocorre ao substituirmos D6 por 7, D7 por 7, E6 por 5 e E7 por 2.

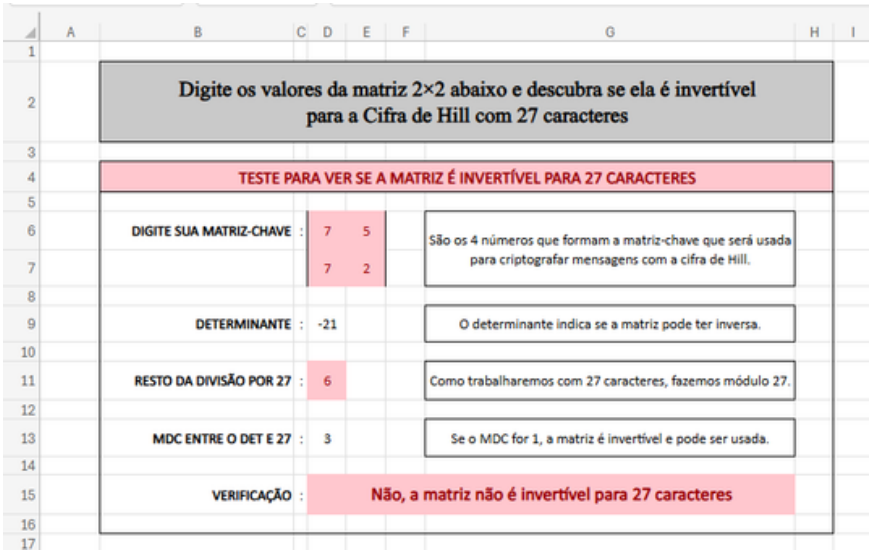


Imagem 1.2. Matriz não invertível módulo 27.

Automaticamente, a planilha calcula o determinante da matriz na célula D11, através de fórmula “=D6E7-E6D7”, isto é, fazendo a diferença entre os produtos da diagonal principal e da diagonal secundária. Neste exemplo, o determinante ficou “-21”.

Ocorre que, para poder ser utilizada como matriz-chave no processo da Cifra de Hill com 27 caracteres, é necessário que o seu determinante, em módulo 27, seja primo com 27, ou seja, que o máximo divisor comum (MDC) entre os dois seja igual a 1.

Por isso, na célula D11 foi implementada a fórmula “=MOD(D9;27)”, que gera o resto da divisão do determinante, anteriormente calculado, por 27. Neste caso, gerando o resultado “6”, o professor pode instruir os alunos a fazerem essa verificação ao somar 27 quantas vezes forem necessárias ao determinante, até encontrar um valor inteiro positivo, como no exemplo -21+27=6.

Em seguida, na célula D13, através da fórmula “=MDC(D11;27)” é calculado o MDC entre 6 e 27, que deu “3”. Como esse MDC é diferente de 1, a matriz é dita não invertível módulo 27 e a planilha

troca as cores para vermelho e informa a seguinte mensagem: “Não, a matriz não é invertível para 27 caracteres”

Para poder prosseguir basta fazer alterações nas entradas da matriz até que a planilha alerte uma que seja viável ao processo. Uma opção é, por exemplo, Trocar o valor da célula D6 para 3, veja abaixo.

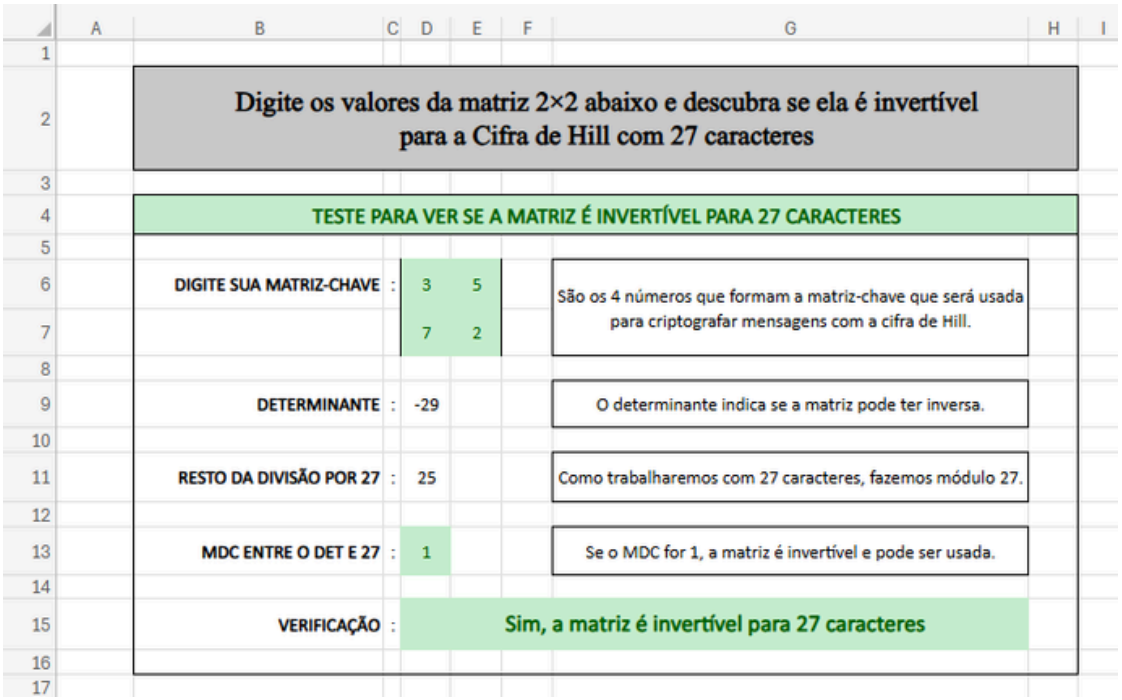


Imagem 1.3. Matriz invertível módulo 27.

Como o determinante, neste caso, deu 1, a planilha troca as cores para verde e informa a seguinte mensagem: “Sim, a matriz é invertível para 27 caracteres”. O que significa que o usuário pode utilizar essa matriz para criptografar mensagens na próxima planilha.

A fim de garantir a segurança dos próximos capítulos continuaremos a utilizar a matriz-chave da Imagem 1.3.

Capítulo II

Hora de Codificar

Transformando Palavras em Códigos Secretos

"Tudo é número" - Pitágoras

Agora que sua matriz de codificação está pronta e segura, é hora de colocar a criptografia em ação. Nesta etapa, cada letra da sua mensagem será convertida em um código matemático único, seguindo as regras definidas pela sua matriz. É como trocar o idioma comum por uma língua secreta, compreendida apenas por quem possui a chave correta para decifrá-la.

Ao longo deste capítulo, você vai aprender a inserir sua mensagem na planilha de criptografia, acompanhar a transformação passo a passo e entender como a matemática garante que seu texto original se torne praticamente indecifrável para curiosos.

AFINAL, AQUI, CADA PALAVRA CONTA
E CADA NÚMERO GUARDA UM SEGREDO

2.1 Conhecendo a Segunda Planilha: Codificação

Esta segunda planilha pretende ser um auxílio completo para a codificação de mensagens de até 16 caracteres, desde a primeira transformação da mensagem em números pré-definidos até as multiplicações de matrizes e construção da mensagem já codificada.

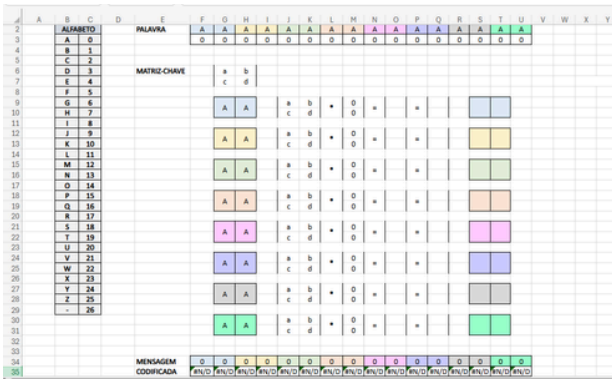


Imagem 2.1. Interface da planilha “Codificação”.

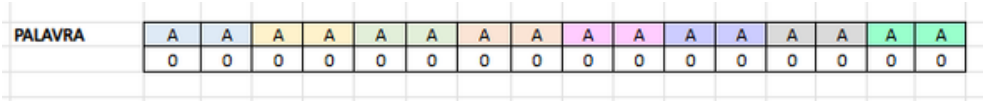
No lado esquerdo da tela da Imagem 2.1 há o alfabeto a ser utilizado em todo o processo. Ele foi composto por 27 caracteres, sendo estas as 26 letras do alfabeto brasileiro mais o caractere "-", que funciona como um espaço entre palavras e também para completar frases com número ímpar de caracteres. A Imagem 2.2 a seguir mostra melhor essa disposição.

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

Imagem 2.2. Alfabeto com 27 caracteres.

De A a Z foram distribuídos os números de 0 a 25, de acordo com a ordem do próprio alfabeto brasileiro, sendo A=0 e Z=25, já para o "-" foi atribuído o valor 26.

No canto superior da planilha há os espaços para escrita da mensagem a ser codificada (Ver Imagem 2.1). As células devem ser preenchidas apenas com as informações contidas na tabela da Imagem 2.2 e a planilha fará a conversão dos sinais informados para os respectivos números, automaticamente.



PALAVRA	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Imagem 2.3. Local de inserção da mensagem inicial.

Abaixo dessa área encontra-se o local de inserção da matriz-chave já verificada na primeira planilha. Inicialmente, a matriz apresenta as entradas "a", "b", "c" e "d", que devem ser substituídas pelos números da matriz que ser quer utilizar (ver Imagem 2.4).

MATRIZ-CHAVE		a	b
		c	d

Imagem 2.4. Local de inserção da matriz-chave.

No centro da planilha está localizado o ambiente em que ocorrerá toda a transformação, já com comandos pré-definidos e que iremos conhecer nas próximas seções deste capítulo. Mas, por hora, observe esse ambiente na Imagem 2.5.

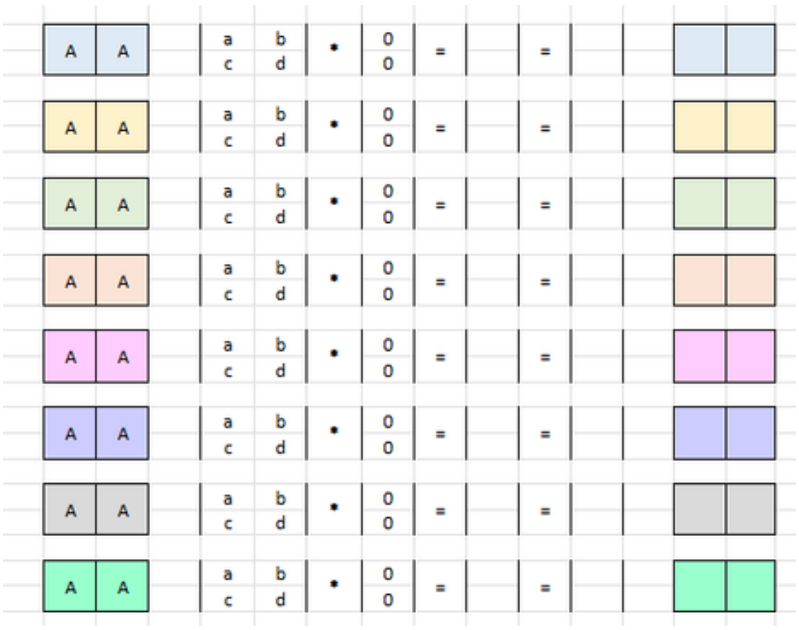


Imagem 2.5. Ambiente de transformação da mensagem.

Note que, desde o ambiente de inserção da mensagem, a mesma encontra-se separada por 8 cores, cada par de letra está representado por uma cor diferente. Isso ocorre devido à escolha de fazer a transformação da mensagem com uma matriz-chave de ordem dois, pois, assim, a mensagem precisa ser codificada a cada par de letras.

No ambiente de transformação da mensagem (Imagem 2.5) é possível ver de forma mais clara essa separação, pois a planilha aponta, ao lado esquerdo, cada dupla de caracteres e, ao lado direito, irá gerar a nova dupla de caracteres que irá substituir as iniciais.

Todo o processo ocorre por meio de multiplicações de matrizes e também da "redução" dos resultados ao módulo 27. Essas funções irão ocorrer na parte central do espaço e como mencionado anteriormente, serão executadas por meio de alguns comandos já programados.

Por fim, a planilha conta com uma parte inferior que "monta" a mensagem codificada ao final do processo.

2.2 Escolhendo a mensagem

Volte sua atenção novamente ao canto superior dessa planilha. Você, como usuário dela, pode digitar letra por letra da mensagem ou, simplesmente, selecionar a letra desejada no cursor que aparece ao clicar em cada célula. Perceba que, sem perda de originalidade da mensagem, ela só pode ser composta por letras maiúsculas.

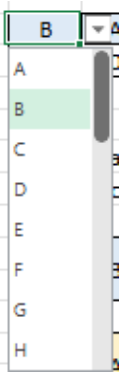


Imagem 2.5. Cursor de seleção de letra.

A mensagem não precisa ter necessariamente todos os 16 caracteres, mas é importante que ela tenha um número par de símbolos; caso não tenha, deve-se acrescentar o ícone "-" ao final, para ajustar ao modelo.

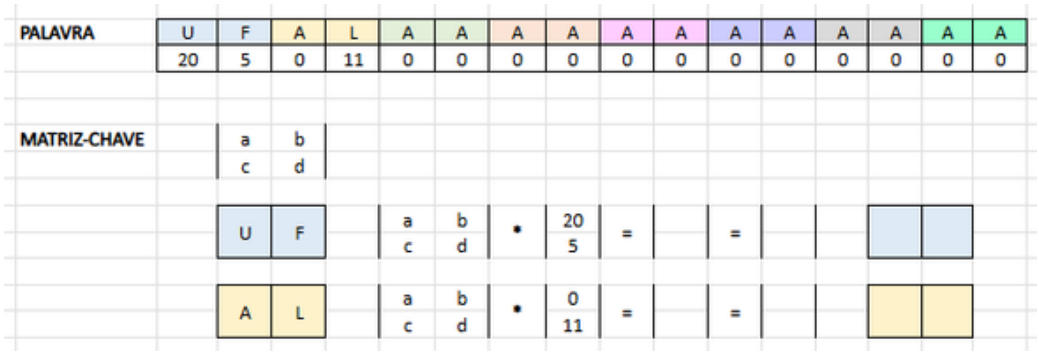


Imagem 2.6. Iserção da palavra "UFAL".

Na Imagem 2.6 tem-se a adição da mensagem “UFAL” à planilha. Essa mensagem contém 4 letras, isto é, um número par de letras, tornando possível a separação delas em dois pares no ambiente de transformação da mensagem, os pares “UF” e “AL”. Perceba também que a planilha faz essa separação de forma automática.

Em contrapartida, a mensagem “PROFMAT” tem 7 letras, por ser um número ímpar, a última letra não teria um par, por isso acrescentamos o espaço (representado por “-”) e optamos por usar a mensagem “PROFMAT-”. Veja a Imagem 2.7.

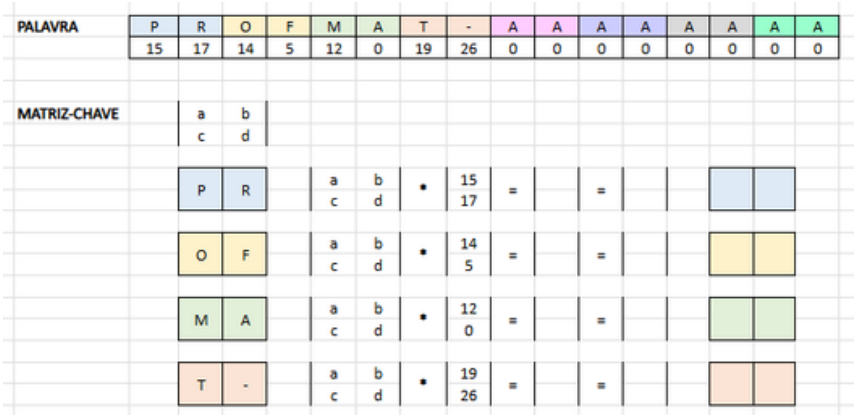


Imagem 2.7. Iserção da palavra “PROFMAT-”.

É perceptível que, ao inserir ambas as mensagens, a planilha faz a conversão automática das letras para os respectivos números. Essa função está ativada a partir da utilização da fórmula “PROCV”, e não pode ser alterada pelos usuários, já que a planilha está restrita para que os usuários só possam modificar uma quantidade limitada de células.

A fim de exemplificar a codificação de uma mensagem de 16 letras, utilizaremos a frase “UFAL-PROFMAT-IM-” a partir de agora.

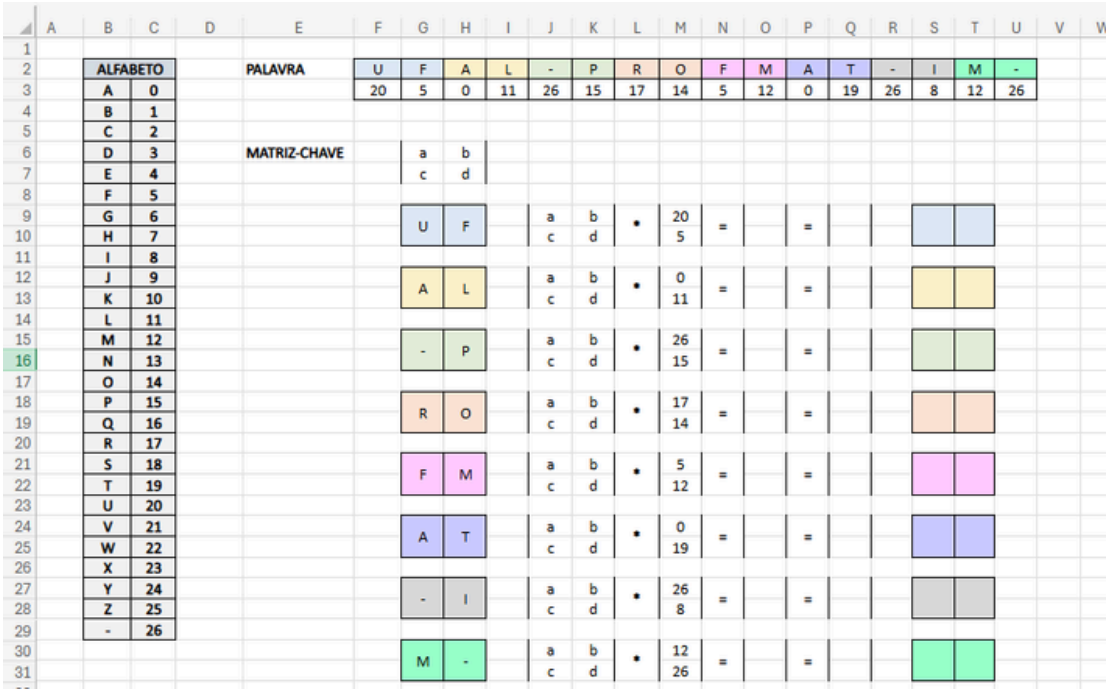


Imagem 2.8. Mensagem “UFAL-PROFMAT-IM-”

Ao dispor da frase completa, a planilha faz a conversão para os números e já converte as duplas de símbolos para uma matriz coluna de seus números. Como, por exemplo, “UF” que nas células M9 e M10 tem sua representação matricial.

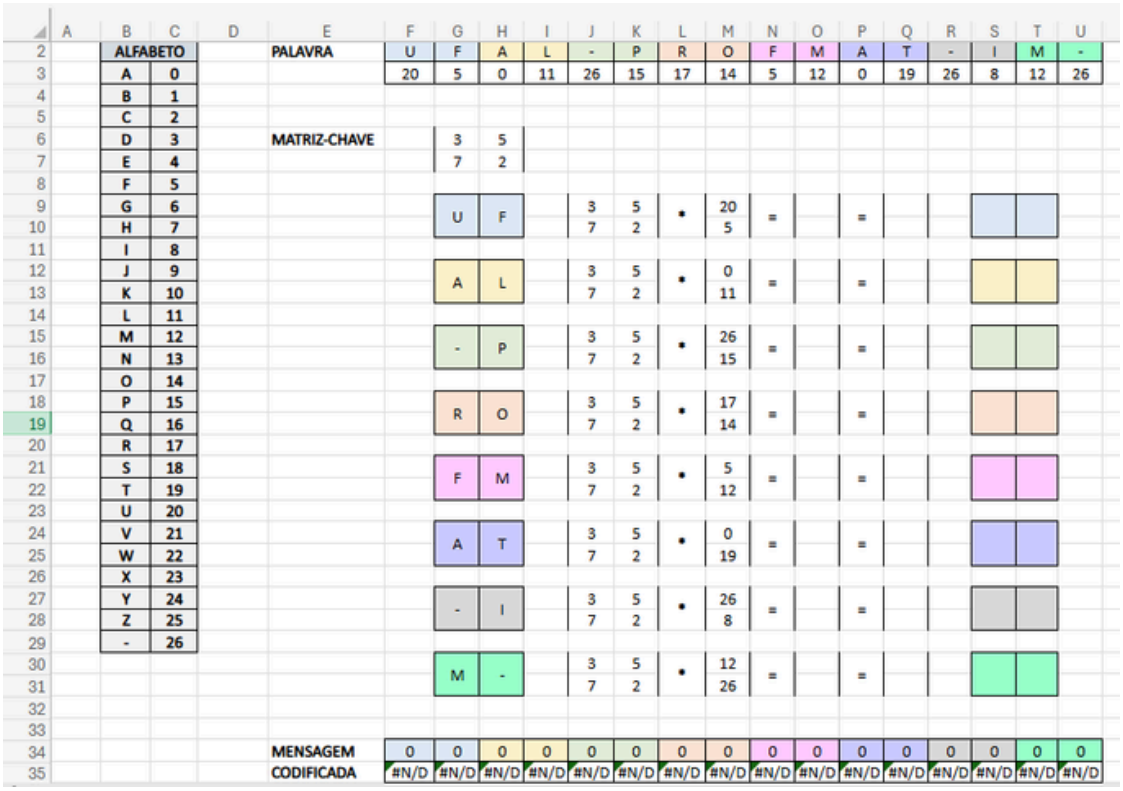
2.3 Codificando a mensagem

Na etapa atual o primeiro passo é atribuir a matriz-chave já verificada. A planilha irá substituir no mesmo instante todas as matrizes no ambiente de transformação da mensagem.

A exemplo, na imagem 2.8, adotamos a matriz-chave já verificada no capítulo I deste manual, cujas entradas são 3, 5, 7 e 2.

É importante sempre lembrar de verificar antes, pois, embora qualquer matriz de ordem 2 possa ser colocada nessa etapa, matrizes

que não são invertíveis módulo 27 serão incapazes de servir para recuperar a mensagem codificada.



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

PALAVRA	U	F	A	L	-	P	R	O	F	M	A	T	-	I	M	-
	20	5	0	11	26	15	17	14	5	12	0	19	26	8	12	26
MATRIZ-CHAVE		3	5													
		7	2													
	U	F			3	5	•	20	=		=					
					7	2		5								
	A	L			3	5	•	0	=		=					
					7	2		11								
	-	P			3	5	•	26	=		=					
					7	2		15								
	R	O			3	5	•	17	=		=					
					7	2		14								
	F	M			3	5	•	5	=		=					
					7	2		12								
	A	T			3	5	•	0	=		=					
					7	2		19								
	-	I			3	5	•	26	=		=					
					7	2		8								
	M	-			3	5	•	12	=		=					
					7	2		26								
MENSAGEM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CODIFICADA	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D

Imagem 2.9. Matriz-chave substituida

A ideia da planilha é justamente reduzir processos demasiadamente extensos para permitir o foco no processo e em como utilizar a ferramenta de forma adequada.

Assim, ao colocar a matriz-chave, a planilha já irá efetuar todo o processo de codificação, como é possível observar na Imagem 2.10 abaixo. Nessa mesma imagem, note que é fundamental que o professor atue como mediador nessa parte, para que os alunos direcionem a atenção para o processo ao qual o Excel codificou a mensagem.

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

MATRIZ-CHAVE

3	5
7	2

PALAVRA	U	F	A	L	-	P	R	O	F	M	A	T	-	I	M	-
	20	5	0	11	26	15	17	14	5	12	0	19	26	8	12	26

U	F		3	5	•	20	=	85	=	4		E	P
			7	2		5		150		15			
A	L		3	5	•	0	=	55	=	1		B	W
			7	2		11		22		22			
-	P		3	5	•	26	=	153	=	18		S	X
			7	2		15		212		23			
R	O		3	5	•	17	=	121	=	13		N	M
			7	2		14		147		12			
F	M		3	5	•	5	=	75	=	21		V	F
			7	2		12		59		5			
A	T		3	5	•	0	=	95	=	14		O	L
			7	2		19		38		11			
-	I		3	5	•	26	=	118	=	10		K	J
			7	2		8		198		9			
M	-		3	5	•	12	=	166	=	4		E	B
			7	2		26		136		1			

MENSAGEM CODIFICADA	E	P	B	W	S	X	N	M	V	F	O	L	K	J	E	B
	4	15	1	22	18	23	13	12	21	5	14	11	10	9	4	1

Imagem 2.10. Mensagem Codificada.

Dessa forma, a mensagem original “UFAL-PROFMAT-IM-” virou a mensagem codificada “EPBWSXNMVFOLKJEB”.

MENSAGEM CODIFICADA	E	P	B	W	S	X	N	M	V	F	O	L	K	J	E	B
	4	15	1	22	18	23	13	12	21	5	14	11	10	9	4	1

Imagem 2.11. Mensagem final codificada.

Agora que sua mensagem foi transformada em um enigma matemático, é hora de guardá-la com segurança. Nos próximos capítulos, vamos revelar o caminho inverso: como decodificar cada número e recuperar o texto original, letra por letra. A missão está apenas começando.

Capítulo III

Quebrando o Código

Montando a Chave para Desvendar Mensagens

"A única forma de aprender Matemática é fazendo Matemática" - Paul Halmoss

Capítulo III
Quebrando o código

Depois de aprender a transformar palavras em códigos secretos, chegou a hora de dar o próximo passo: desvendar as mensagens codificadas. Para isso, precisamos encontrar uma ferramenta especial, a matriz de decodificação.

Neste capítulo, você vai aprender a "quebrar o código" seguindo um método passo a passo. Usaremos nossa terceira planilha interativa para calcular o determinante, identificar o inverso multiplicativo e construir a matriz que permite transformar códigos aparentemente indecifráveis em palavras compreensíveis. Prepare-se como um detetive que junta pistas para solucionar um mistério.

REUNA NÚMEROS, FÓRMULAS E CONCEITOS MATEMÁTICOS
MONTE A CHAVE QUE REVELA SEGREDOS

3.1 Conhecendo a Terceira Planilha: Matriz de decodificação

A terceira planilha, intitulada "Matriz de decodificação" serve para encontrar a matriz de decodificação com base na matriz-chave que foi usada para codificar a mensagem anteriormente,

Ela conduz o processo de forma simples e organizada, dividindo-o em três etapas: na Parte 1, você insere os números da matriz-chave e obtém automaticamente o determinante e seu valor módulo 27; na Parte 2, identifica-se o inverso multiplicativo do determinante, fundamental para o cálculo da inversa; e na Parte 3, a planilha combina a matriz adjunta com esse inverso para gerar a matriz de decodificação, que permitirá reverter o código e recuperar a mensagem original. Observe na Imagem 3.1.

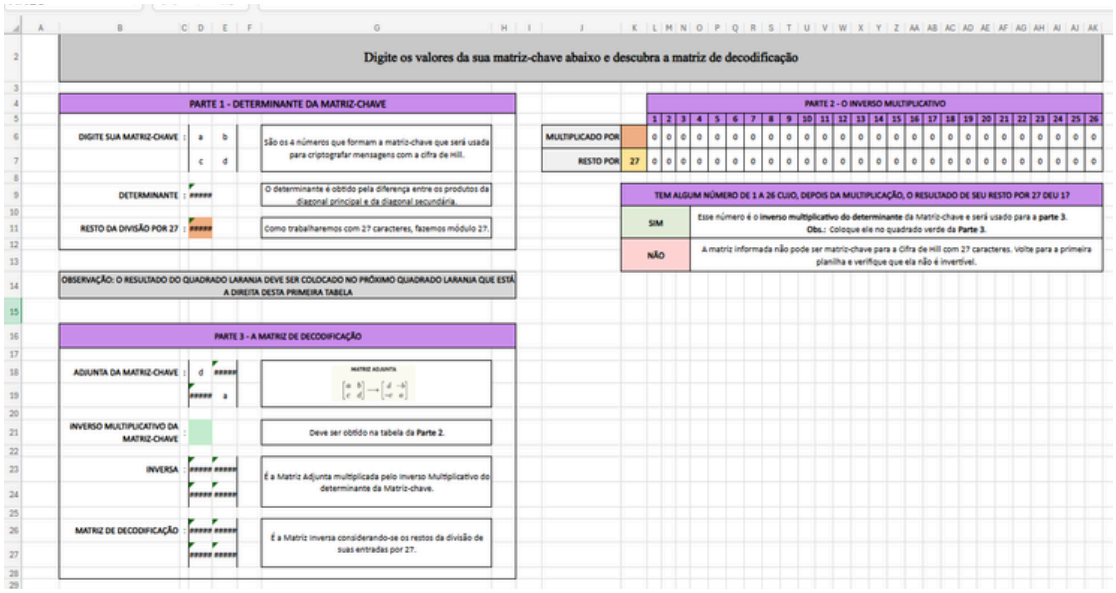


Imagem 3.1. Interface da planilha “Matriz de Decodificação”.

A tabela da parte superior esquerda é a primeira a ser utilizada. Nela, basta digitar a matriz-chave de codificação nas células D6, D7, E6 e E7.

De forma similar a da primeira planilha (Ver no Capítulo I), ao informar as entradas da matriz-chave, a interface está programada para calcular, automaticamente, o determinante dessa matriz e aplicar o módulo 27 a esse determinante, o segundo de forma a procurar pelo “Resto da divisão por 27”. Na Imagem 3.2 encontra-se a aplicação dessa etapa para a matriz de referência que está sendo utilizada desde o primeiro capítulo deste manual.

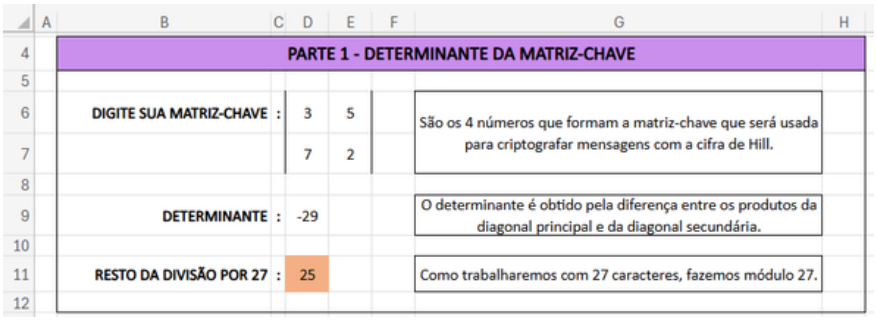


Imagem 3.2. Parte 1 - Determinante da Matriz-chave.

Diante dessa aplicação, a tabela gera o produto final na casa D11, que, nesse caso em específico, foi o número 25. O resultado dessa célula, já destacado no tom laranja, representa o resto da divisão por 27 do determinante da matriz-chave e deve ser utilizado como ponto de partida na próxima tabela da planilha.

A segunda tabela também contém uma célula na cor laranja, a K6. O resultado final da Tabela 1 deve ser posto nessa casa e, após essa alteração, a tabela irá verificar imediatamente qual dos números de 0 a 26 é inverso multiplicativo desse valor, isto é, qual deles gera resultado igual a 1 em módulo 27 quando multiplicado pelo valor especificado.

	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK
4			PARTE 2 - O INVERSO MULTIPLICATIVO																									
5			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
6	MULTIPLICADO POR	25	25	50	75	100	125	150	175	200	225	250	275	300	325	350	375	400	425	450	475	500	525	550	575	600	625	650
7	RESTO POR	27	25	23	21	19	17	15	13	11	9	7	5	3	1	26	24	22	20	18	16	14	12	10	8	6	4	2

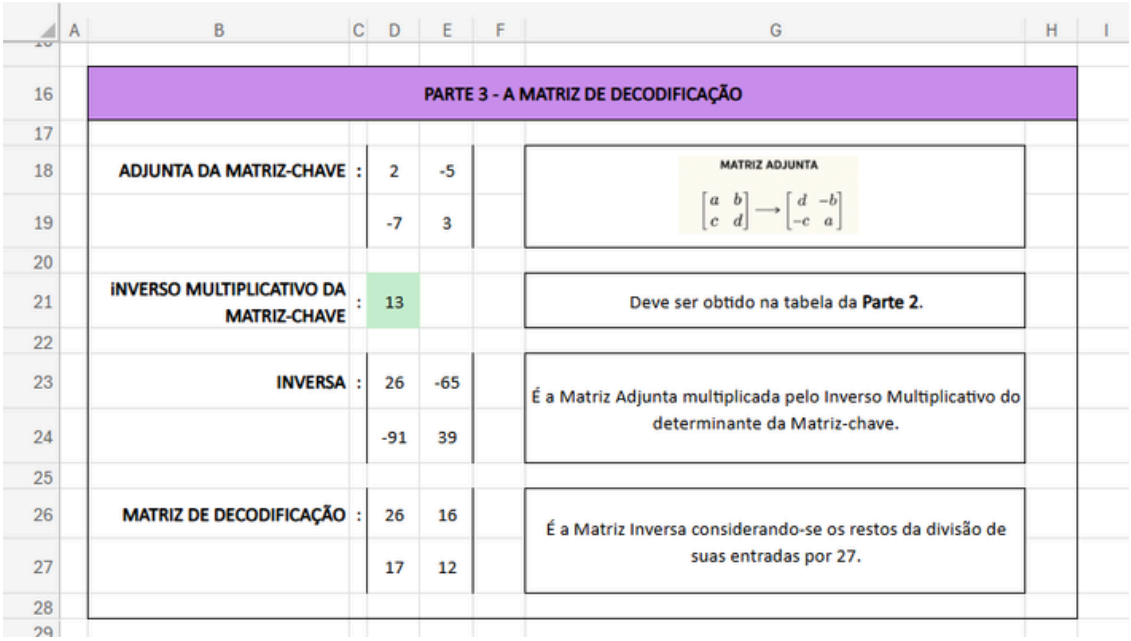
Imagem 3.3. Parte 2 - O inverso multiplicativo.

Na Imagem 3.3 está apontado, em verde, o inverso multiplicativo para o 25, o inverso é o número 13. Ocorre que, para cada número haverá um inverso multiplicativo diferente e a tabela aponta de modo automático esse número, através da coloração verde.

Nessa parte o cuidado foi o de transformar um conceito muito específico do trabalho com a aritmética modular em algo visual para que um estudante de Ensino Médio possa compreender o processo. Então, mediante o auxílio do professor, o aluno irá fazer a verificação de todas as multiplicações nessa tabela, verificando cada caso e que só há um número, dentre as opções disponíveis, que seja inverso multiplicativo para a matriz-chave informada.

Na próxima tabela, a da Parte 3 da planilha, há uma célula nesse mesmo tom esverdeado. Nela, deve-se pôr o inverso multiplicativo encontrado na Tabela 2, que será usado para enfim gerar a matriz de decodificação.

Além disso, a Parte 3 conta também com a adjunta da matriz-chave que, unida ao inverso multiplicativo, gerará, como resultado final, a inversa da matriz-chave, a tão esperada matriz de decodificação. Esse processo está disponível na Imagem 3.4 a seguir.



PARTE 3 - A MATRIZ DE DECODIFICAÇÃO				
ADJUNTA DA MATRIZ-CHAVE :	2	-5	MATRIZ ADJUNTA $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \rightarrow \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	
	-7	3		
INVERSO MULTIPLICATIVO DA MATRIZ-CHAVE :	13		Deve ser obtido na tabela da **Parte 2**.	
INVERSA :	26	-65	É a Matriz Adjunta multiplicada pelo Inverso Multiplicativo do determinante da Matriz-chave.	
	-91	39		
MATRIZ DE DECODIFICAÇÃO :	26	16	É a Matriz Inversa considerando-se os restos da divisão de suas entradas por 27.	
	17	12		

Imagem 3.3. Parte 3 - A matriz de decodificação.

A tabela apresenta rapidamente a adjunta da matriz-chave, pois ela já pega como referência as entradas da matriz posta pelo estudante na Tabela 1, então ele consegue acompanhar esse processo de forma conjunta, porém, para um auxílio maior, ao lado direito da adjunta há uma explicação sobre a mesma.

Ademais, ao colocar o valos do inverso multiplicativo, a tabela faz

a multiplicação pela adjunta e já expressa também essa matriz pelo módulo 27, como a “matriz de decodificação”, que nada mais é do que a inversa módulo 27 da matriz-chave.

3.2 Conhecendo a Planilha Extra: Decodificação

Essa planilha não ganhou um capítulo só para si porque ela é, essencialmente, a planilha dois, a de codificação. Sua estrutura é igual a da anterior, mudando apenas “matriz-chave” para “matriz de decodificação” e “mensagem codificada” para “mensagem decodificada.

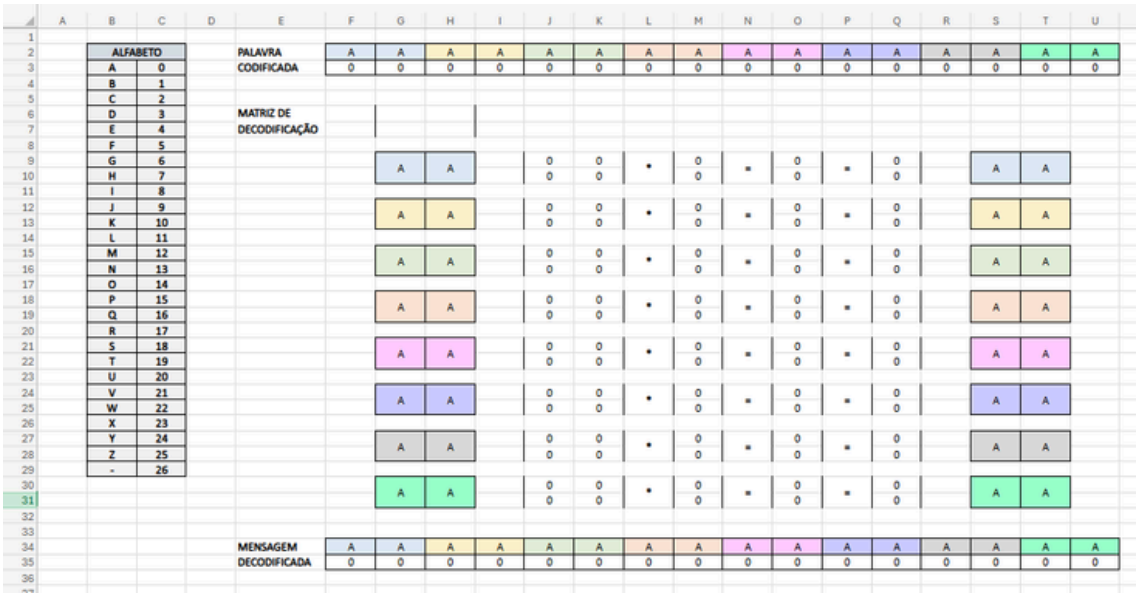
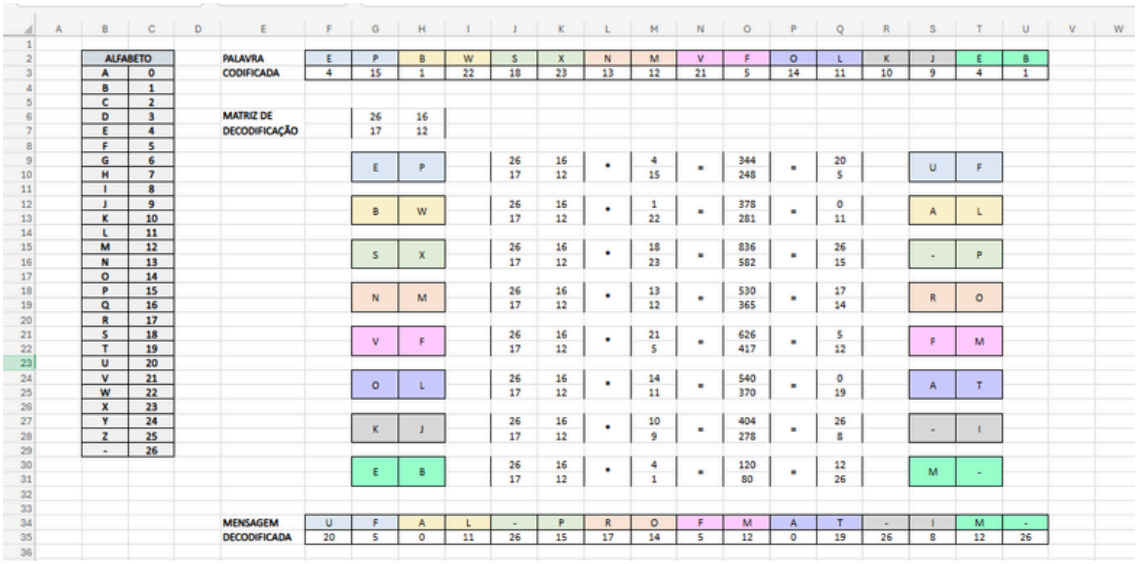


Imagem 3.4. Planilha extra: ambiente de decodificação de mensagem.

Ela serve de apoio para a verificação da decodificação da mensagem, sem excluir o progresso feito na Planilha 2, tendo em vista sua separação da mesma. Observe na Imagem 3.5, nela utilizamos a men-

sagem codificada no Capítulo 2 e a matriz de decodificação encontrada na Seção 3.1 deste capítulo.



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

PALAVRA CODIFICADA	E	P	B	W	S	X	N	M	V	F	O	L	K	J	E	B
	4	15	1	22	18	23	13	12	21	5	14	11	10	9	4	1

MATRIZ DE DECODIFICAÇÃO

26	16
17	12

MENSAGEM DECODIFICADA	U	F	A	L	-	P	R	O	F	M	A	T	-	I	M	-
	20	5	0	11	26	15	17	14	5	12	0	19	26	8	12	26

Imagem 3.4. Mensagem decodificada.

Assim, fica fácil verificar que conseguimos retomar a mensagem original e compreender todo o processo por trás disso.

Capítulo IV

O Impasse do Módulo 27

Quando a Cifra Trava

"A Matemática não mente. Mente quem faz mau uso dela."
- Albert Einstein

Depois de aprender a transformar palavras em códigos secretos, chegou a hora de discutirmos o que ocorre quando usamos uma matriz que não é invertível módulo 27. Será que o processo de codificação e decodificação permanece possível? Neste capítulo, investigaremos esse impasse matemático e compreenderemos por que a invertibilidade não é apenas um detalhe técnico, mas o elemento que garante a segurança e a recuperação fiel das mensagens.

NEM TODO CÓDIGO ENCONTRA O CAMINHO DE VOLTA
A INVERTIBILIDADE É A CHAVE

4.1 Codificando sem Inversão

Voltemos a observar a matriz da Imagem 1.2 (abaixo, na Imagem 4.1), matriz essa que não é invertível para o módulo 27.

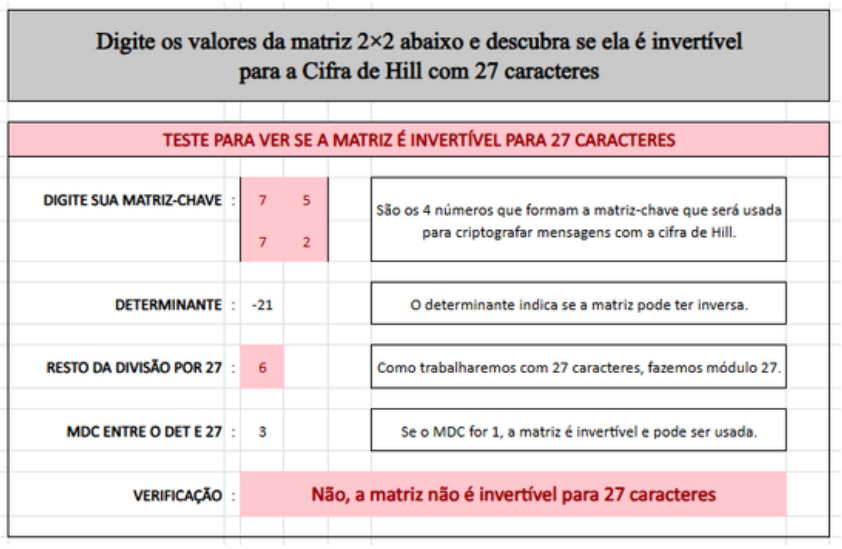
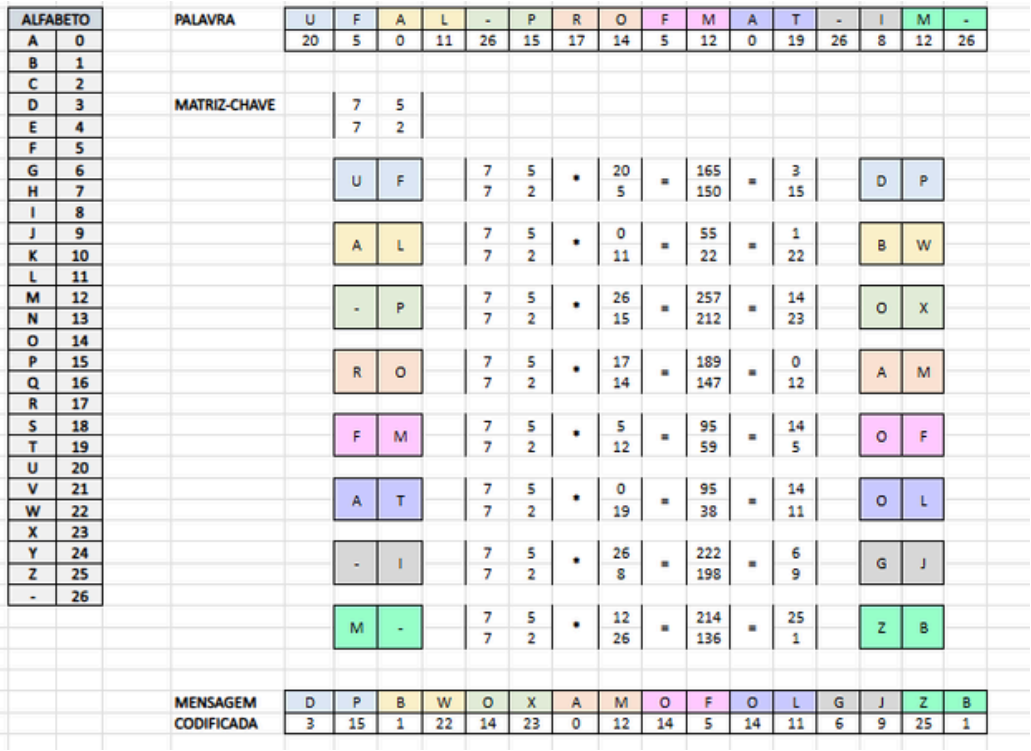


Imagem 4.1. Matriz não invertível em módulo 27.

Por curiosidade, um aluno, mesmo com a instrução da primeira planilha, pode querer continuar a utilizar essa matriz. O próximo

passo desse estudante será codificar uma mensagem na segunda planilha. Aqui utilizaremos da mesma mensagem já codificada nos capítulos anteriores, mas, dessa vez, utilizaremos da matriz não invertível para codificá-la, vejamos o que ocorre no ambiente de codificação da mensagem, sob essas circunstâncias, na Imagem 4.2.



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

PALAVRA	U	F	A	L	-	P	R	O	F	M	A	T	-	I	M	-
	20	5	0	11	26	15	17	14	5	12	0	19	26	8	12	26

MATRIZ-CHAVE

7	5
7	2

U	F	7 7	5 2	•	20 5	=	165 150	=	3 15					D	P	
A	L	7 7	5 2	•	0 11	=	55 22	=	1 22					B	W	
-	P	7 7	5 2	•	26 15	=	257 212	=	14 23					O	X	
R	O	7 7	5 2	•	17 14	=	189 147	=	0 12					A	M	
F	M	7 7	5 2	•	5 12	=	95 59	=	14 5					O	F	
A	T	7 7	5 2	•	0 19	=	95 38	=	14 11					O	L	
-	I	7 7	5 2	•	26 8	=	222 198	=	6 9					G	J	
M	-	7 7	5 2	•	12 26	=	214 136	=	25 1					Z	B	

MENSAGEM CODIFICADA	D	P	B	W	O	X	A	M	O	F	O	L	G	J	Z	B
	3	15	1	22	14	23	0	12	14	5	14	11	6	9	25	1

Imagem 4.2. Codificação da mensagem com a nova matriz.

A mensagem foi aparentemente codificada, de fato, a mensagem “UFAL-PROFMAT-IM-” tornou-se “DPBWOXAMOFOLGJZB”. Dessa forma, o estudante pode até achar que deu certo e que “quebrou” o código, afinal, a mensagem foi transformada em outra que é irreconhecível, entretanto, agora ele terá que verificar qual a matriz que pode ser usada para recuperar a mensagem, sigamos então para a terceira planilha na Imagem 4.3.

PARTE 1 - DETERMINANTE DA MATRIZ-CHAVE			
DIGITE SUA MATRIZ-CHAVE :	7	5	São os 4 números que formam a matriz-chave que será usada para criptografar mensagens com a cifra de Hill.
	7	2	
DETERMINANTE :	-21		O determinante é obtido pela diferença entre os produtos da diagonal principal e da diagonal secundária.
RESTO DA DIVISÃO POR 27 :	6		Como trabalharemos com 27 caracteres, fazemos módulo 27.

OBSERVAÇÃO: O RESULTADO DO QUADRADO LARANJA DEVE SER COLOCADO NO PRÓXIMO QUADRADO LARANJA QUE ESTÁ A DIREITA DESTA PRIMEIRA TABELA

Imagem 4.3. Parte 1, inserindo a matriz na planilha

Como visto no Capítulo 3 deste manual, essa primeira parte da planilha serve para obter o determinante da matriz de codificação para prosseguir com a obtenção da matriz de decodificação, acompanhemos, na Imagem 4.4, essa transformação na parte 2, aplicando o valor "6" da célula destacada em laranja na próxima parte, também em uma célula destacada na mesma cor.

		PARTE 2 - O INVERSO MULTIPLICATIVO																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
MULTIPLICADO POR	6	6	12	18	24	30	36	42	48	54	60	66	72	78	84	90	96	102	108	114	120	126	132	138	144	150	156
RESTO POR	27	6	12	18	24	3	9	15	21	0	6	12	18	24	3	9	15	21	0	6	12	18	24	3	9	15	21

TEM ALGUM NÚMERO DE 1 A 26 CUJO, DEPOIS DA MULTIPLICAÇÃO, O RESULTADO DE SEU RESTO POR 27 DEU 1?	
SIM	Esse número é o **inverso multiplicativo do determinante** da Matriz-chave e será usado para a **parte 3**. **Obs.:** Coloque ele no quadrado verde da **Parte 3**.
NÃO	A matriz informada não pode ser matriz-chave para a Cifra de Hill com 27 caracteres. Volte para a primeira planilha e verifique que ela não é invertível.

Imagem 4.4. Parte 2, tentando encontrar o inverso multiplicativo.

É aqui que o processo apresenta sua falha, ocorre que não há nenhum número que, ao ser multiplicado por 6 e, em seguida, ao ser dividido por 27 dará resto 1. Assim, a matriz não tem inverso multiplicativo e, dessa forma, também não há como encontrar uma matriz de decodificação, tendo em vista que essa matriz tem que ser resultante da multiplicação do inverso multiplicativo pela adjunta da matriz inicial.

No próximo capítulo, exploraremos como esses conceitos podem ser levados à sala de aula e como situações específicas — como o uso da matriz identidade — podem se transformar em oportunidades de reflexão e aprendizagem sobre o papel das matrizes na criptografia.

Capítulo V

Desdobramentos Pedagógicos

Decifre-me Se For Capaz

"Forasteiro — respondeu o Homem que Calculava —, não censuro a curiosidade que te levou a perturbar a marcha de meus cálculos e a serenidade dos meus pensamentos."

- Malba Tahan em "O Homem que Calculava"

Capítulo V
Desdobramentos Pedagógicos

Nos capítulos anteriores, apresentamos as bases matemáticas da Cifra de Hill e exploramos, passo a passo, as planilhas desenvolvidas no Excel para automatizar processos como codificação, decodificação e análise de matrizes no módulo 27. Esses materiais foram construídos para tornar os procedimentos mais acessíveis, organizados e visualmente claros, permitindo que o professor compreenda a lógica por trás de cada etapa.

Chegado este ponto, é hora de deslocar o olhar: das ferramentas para a sala de aula. Neste capítulo, discutiremos como utilizar essas planilhas de forma pedagógica, criando oportunidades de investigação, experimentação e construção de sentido por parte dos estudantes. A criptografia aparece aqui não apenas como contexto motivador, mas como recurso metodológico capaz de integrar tecnologia, raciocínio matemático e resolução de problemas.

Com isso, buscamos mostrar que a matemática pode ser vivida, manipulada e descoberta — e não apenas aplicada mecanicamente.

QUANDO A FERRAMENTA SE TORNA PONTE
A MATEMÁTICA ENCONTRA O ESTUDANTE

5.1 Decifre-me se for capaz

Desafiar a lógica e a interpretação é o ponto de partida deste enigma. Nele, decifrar é mais do que resolver, é compreender os caminhos ocultos do raciocínio matemático daquele que decifrou a mensagem em primeiro lugar. A provocação lógica assemelha-se a um caça palavras, diferenciado apanas pelo fatos de que, primeiramente, as palavras dispostas no jogo estão codificadas e, posteriormente, pelo fato de que toda a tabela representa uma única mensagem completa. Observe um modelo desse desafio na Imagem 5.1.

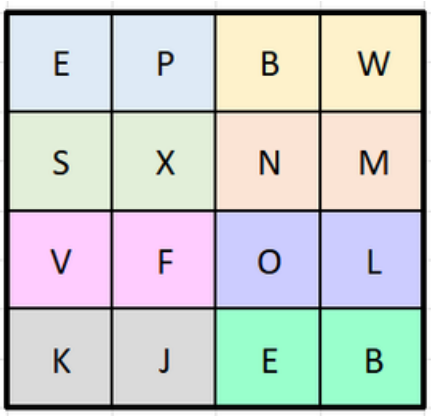


Imagem 5.1. Caça-palavras criptografado com uma matriz-chave de ordem 2.

O caça-palavras codificado tem como objetivo levar os estudantes a entender, para o além de somente aplicar as planilhas. Isto é, além de compreender sua utilização, usá-la como artificio para a construção do conhecimento e como auxílio para a solução do problema que o envolve: encontrar a matriz de codificação de uma mensagem para poder decodificá-la por completo.

Na Imagem 5.1, encontra-se o caça-palavras criptografado com a mesma mensagem utilizada nos capítulos anteriores, a modelo de exemplificação. Como a mensagem foi criptografada com uma matriz-chave de ordem 2, é necessário saber ao menos 2 blocos, de 2 caracteres cada, da mensagem original. Assim, imagine que, neste exemplo, apenas sabemos que, em alguma linha do tabuleiro, encontra-se criptografada a palavra “UFAL” e que todas as linhas juntas formam uma mensagem legitima, isto é, uma mensagem compreensível na lingua portuguesa.

Alguns conhecimentos prévios sobre as condições de codificação da mensagem precisam fazer parte da consciência comum dos desafiados, para que haja a possibilidade de resolução, são elas:

1. A mensagem foi codificada pela utilização da Cifra de Hill;
2. O alfabeto utilizado contém 27 caracteres, sendo os 26 primeiros as letras do alfabeto latino e o 27º o caractere Hífen (-);
3. A matriz chave utilizada é de ordem 2;
4. As entradas da matriz chave são números naturais menores ou iguais a 10;
5. Cada parte da mensagem está disponibilizada em uma linha da tabela;
6. Cada linha deve ser lida da esquerda para a direita.

Assim, vamos começar a solucionar esse quebra-cabeça lógico. Consideremos primeiramente a matriz M abaixo como a nossa matriz-chave de ordem 2 genérica, isto é, a matriz que não conhecemos suas entradas, mas que foi utilizada para codificar a mensagem original. O objetivo aqui é justamente encontrar esses valores para só então conseguir decodificar as mensagens.

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

Por se tratar de uma mensagem já conhecida por nós, sabemos que “UFAL” está escondida na primeira linha do tabuleiro, no entanto, vamos adotar a solução considerando as duas primeiras linhas como possibilidades, para observar o que ocorre quando consideramos que a palavra está escondida em uma linha em que ela não está.

O fato é que, considerando o nosso conjunto alfabético como o descrito no item 2 dos conhecimentos prévios, para qualquer uma das linhas a palavra UFAL dividida nos blocos “UF” e “AL” só tem uma possibilidade de matrizes relacionadas, que está descrita abaixo.

$$\mathrm{UF} \rightarrow \begin{bmatrix} 20 \\ 5 \end{bmatrix} \text{ e } \mathrm{AL} \rightarrow \begin{bmatrix} 0 \\ 11 \end{bmatrix}$$

A primeira linha da tabela é a mensagem “EPBW”, neste caso, consideramos que “UF” virou “EP” e “AL” virou “BW”. Veja abaixo como fica isto consideranto a nossa matriz M.

$$\mathrm{UF} \rightarrow \mathrm{EP} \text{ e } \mathrm{AL} \rightarrow \mathrm{BW}$$

Isto é,

$$\mathrm{EP} \rightarrow \begin{bmatrix} 4 \\ 15 \end{bmatrix} \text{ e } \mathrm{BW} \rightarrow \begin{bmatrix} 1 \\ 22 \end{bmatrix}$$

ou ainda,

$$\mathrm{M} \cdot \mathrm{UF} \equiv \mathrm{EP} \mod 27 \text{ e } \mathrm{M} \cdot \mathrm{AL} \equiv \mathrm{BW} \mod 27$$

Traduzindo isto para o formato matricial:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 15 \end{bmatrix} \mod 27 \text{ e } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 11 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 22 \end{bmatrix} \mod 27$$

$$\Longrightarrow \begin{bmatrix} 20a + 5b \\ 20c + 5d \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 15 \end{bmatrix} \mod 27 \text{ e } \begin{bmatrix} 11b \\ 11d \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 22 \end{bmatrix} \mod 27$$

Em sistemas isto fica:

$$\textbf{(i)}\begin{cases} 20a + 5b \equiv 4 \mod 27 \\ 11b \equiv 1 \mod 27 \end{cases} \text{ e } \textbf{(ii)}\begin{cases} 20c + 5d \equiv 15 \mod 27 \\ 11d \equiv 22 \mod 27 \end{cases}$$

Agora resta apenas resolver os sistemas, lembrando sempre que a congruência em módulo 27 nada mais é do que o resto da divisão por 27. Nesta parte usaremos a tabela 5, que será explicada a medida em que for utilizada. Nesta etapa pode-se utilizar os métodos de solução de sistemas convencionais, no entanto, neste exemplo não será necessário, pois cada sistema apresenta uma de suas duas equivalências com apenas uma incógnita. Começemos então pelo sistema (i), na equivalência mais simples desta.

$$11b \equiv 1 \mod 27$$

Quer se encontrar o número b ao qual, ao multiplicá-lo por 11 e dividí-lo por 27 seu resto será de 1. Para isso irmos utilizar a planilha exposta na Imagem 5.2 abaixo,

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
COEFICIENTE DA ICÓGNITA		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DIVISÃO POR	27	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
QUOCIENTE DA DIVISÃO POR	27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RESTO DA DIVISÃO POR	27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Recurso de apoio para resolver congruências modulares no módulo 27

Observação: Coloque, na célula C6 (amarela), o coeficiente da icógnita.

Imagem 5.2. Apoio ao “Decifre-me se for capaz”.

Esta planilha serve para testar todos os valores prováveis para a incógnica b na equivalência pontada. Para tanto, colocaremos o coeficiente 11 na célula C6 (em amarelo) e iremos verificar em qual caso o resto da divisão por 27 dá 1, como queremos.

Recurso de apoio para resolver equações modulares no módulo 27																										
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
COEFICIENTE DA ICÓGNITA	11	11	22	33	44	55	66	77	88	99	110	121	132	143	154	165	176	187	198	209	220	231	242	253	264	275	286	297
DIVISÃO POR	27	0,41	0,81	1,22	1,63	2,04	2,44	2,85	3,26	3,67	4,07	4,48	4,89	5,30	5,70	6,11	6,52	6,93	7,33	7,74	8,15	8,56	8,96	9,37	9,78	10,19	10,59	11,00
QUOCIENTE DA DIVISÃO POR	27	0	0	1	1	2	2	2	3	3	4	4	4	5	5	6	6	6	7	7	8	8	8	9	9	10	10	11
RESTO DA DIVISÃO POR	27	11	22	6	17	1	12	23	7	18	2	13	24	8	19	3	14	25	9	20	4	15	26	10	21	5	16	0
Observação: Coloque, na célula C6 (amarela), o coeficiente da incógnita.																												

Imagem 5.3. Apoio para coeficiente igual a 11.

Observando a Imagem 5.3 é possível notar que o resto só dará um na célula H9, que ocorre na multiplicação de 11 pelo valor 5, logo, b tem valor 5. Substituindo isto na primeira congruência do sistema (i), obteremos:

$$\begin{aligned} & 20a + 5b \equiv 4 \mod 27 \\ \Longrightarrow\ & 20a + 5 \cdot 5 \equiv 4 \mod 27 \\ \Longrightarrow\ & 20a + 25 \equiv 4 \mod 27 \\ \Longrightarrow\ & 20a \equiv -21 \mod 27 \end{aligned}$$

Como na planilha de apoio no Excel os restos são positivos, basta orientar que sempre que a equivalência resultar em um número negativo como resto some-se quantos 27 forem necessários até encontrar o primeiro inteiro positivo. Neste caso, basta somar 27 apenas uma vez, resultanto em:

$$20a \equiv 6 \mod 27$$

Com o auxilio da planilha, colocando 20 na célula C6 e procurando, na linha 9, o resto igual a 6, obteremos que tem valor igual a 3 (Ver Imagem 5.4).

Recurso de apoio para resolver equações modulares no módulo 27																										
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
COEFICIENTE DA ICÓGNITA	20	20	40	60	80	100	120	140	160	180	200	220	240	260	280	300	320	340	360	380	400	420	440	460	480	500	520	540
DIVISÃO POR	27	0,74	1,48	2,22	2,96	3,70	4,44	5,19	5,93	6,67	7,41	8,15	8,89	9,63	10,37	11,11	11,85	12,59	13,33	14,07	14,81	15,56	16,30	17,04	17,78	18,52	19,26	20,00
QUOCIENTE DA DIVISÃO POR	27	0	1	2	2	3	4	5	5	6	7	8	8	9	10	11	11	12	13	14	14	15	16	17	17	18	19	20
RESTO DA DIVISÃO POR	27	20	13	6	26	19	12	5	25	18	11	4	24	17	10	3	23	16	9	2	22	15	8	1	21	14	7	0
Observação: Coloque, na célula C6 (amarela), o coeficiente da incógnita.																												

Imagem 5.4. Apoio para coeficiente igual a 20.

Resolveremos o sistema (ii) de forma semelhante, começando pela equivalência mais simples.

$$11d \equiv 22 \mod 27$$

Verificando na Imagem 5.3, o valor de d será 2, pois 11 vezes 2 dá 22 e o resto de 22 na divisão por 27 é ele próprio. Substituindo isso na primeira congruência de (ii), obteremos:

$$\begin{aligned} & 20c + 5d \equiv 15 \mod 27 \\ \Longrightarrow\ & 20c + 5 \cdot 2 \equiv 15 \mod 27 \\ \Longrightarrow\ & 20c + 10 \equiv 15 \mod 27 \\ \Longrightarrow\ & 20c \equiv 5 \mod 27 \end{aligned}$$

E, com o auxílio da Imagem 5.4, c tem valor igual a 7, resultando na matriz M igual a:

$$M = \begin{bmatrix} 3 & 5 \\ 7 & 2 \end{bmatrix}$$

Utilizando as planilhas de matriz de decodificação e a de decifrar a mensagem, obtemos, utilizando o mesmo processo dos capítulos anteriores, a mensagem “UFAL-IM-PROFMAT” que, de fato, é a mensagem que estamos utilizando. Mas ainda vamos verificar esse mesmo processo para a segunda linha do caça-palavras.

A segunda linha da tabela é a mensagem “SXNM”, neste caso, consideramos que “UF” virou “SX” e “AL” virou “NM”. Veja abaixo como fica isto considerando a nossa matriz M.

$$\mathrm{UF} \rightarrow \mathrm{SX} \text{ e } \mathrm{AL} \rightarrow \mathrm{NM}$$

Isto é,

$$\mathrm{SX} \rightarrow \begin{bmatrix} 18 \\ 23 \end{bmatrix} \text{ e } \mathrm{NM} \rightarrow \begin{bmatrix} 13 \\ 12 \end{bmatrix}$$

ou ainda,

$$\mathrm{M} \cdot \mathrm{UF} \equiv \mathrm{SX} \mod 27 \text{ e } \mathrm{M} \cdot \mathrm{AL} \equiv \mathrm{MN} \mod 27$$

Traduzindo isto para o formato matricial:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 23 \end{bmatrix} \mod 27 \text{ e } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 11 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 12 \end{bmatrix} \mod 27$$

$$\Longrightarrow \begin{bmatrix} 20a + 5b \\ 20c + 5d \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 23 \end{bmatrix} \mod 27 \text{ e } \begin{bmatrix} 11b \\ 11d \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 12 \end{bmatrix} \mod 27$$

Em sistemas isto fica:

$$(*) \begin{cases} 20a + 5b \equiv 18 \mod 27 \\ 11b \equiv 13 \mod 27 \end{cases} \text{ e } (**) \begin{cases} 20c + 5d \equiv 23 \mod 27 \\ 11d \equiv 12 \mod 27 \end{cases}$$

Começando a resolver pela equivalência mais simples de (*) e comparando com a Imagem 5.3, b, neste caso, tem valor igual a 11 , fazendo a devida substituição na outra equivalência teremos:

$$\begin{aligned} & 20a + 5b \equiv 18 \mod 27 \\ \Longrightarrow\ & 20a + 5 \cdot 11 \equiv 18 \mod 27 \\ \Longrightarrow\ & 20a + 55 \equiv 18 \mod 27 \\ \Longrightarrow\ & 20a \equiv -37 \mod 27 \end{aligned}$$

Somando 27 duas vezes, teremos:

$$20a \equiv 17 \mod 27$$

Dessa forma, pela Imagem 5.4, o valor de a é 13.

Agora, solucionando (**) da mesma forma, obteremos os valores 1 r 6 para as entradas c e d, respectivamente. Gerando a Matriz-chave de codificação abaixo.

$$M = \begin{bmatrix} 13 & 11 \\ 1 & 6 \end{bmatrix}$$

Com esta matriz, voltemos a utilizar as planilhas deste produto. Primeiramente, utilizaremos a planilha de Matriz de decodificação para achar a inversa de M, acompanhe esse processo nas Imagens 5.5, 5.6 e 5.7 abaixo, que seguem o exposto no Capítulo 3 deste manual.

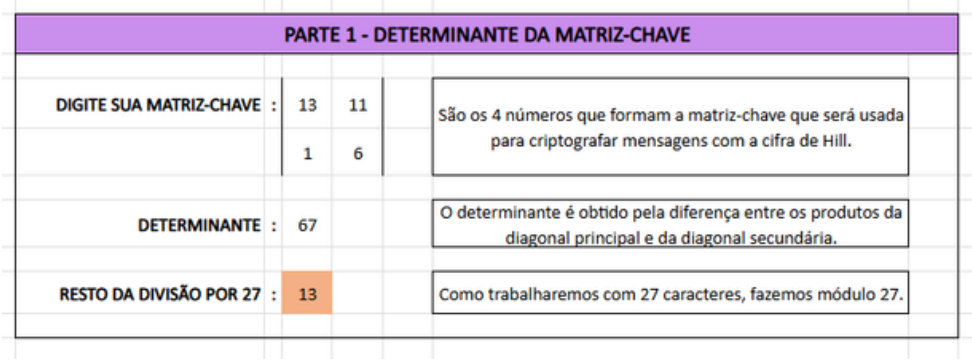


Imagem 5.5. Parte I do processo.

		PARTE 2 - O INVERSO MULTIPLICATIVO																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
MULTIPLICADO POR	13	13	26	39	52	65	78	91	104	117	130	143	156	169	182	195	208	221	234	247	260	273	286	299	312	325	338
RESTO POR	27	13	26	12	25	11	24	10	23	9	22	8	21	7	20	6	19	5	18	4	17	3	16	2	15	1	14

TEM ALGUM NÚMERO DE 1 A 26 CUJO, DEPOIS DA MULTIPLICAÇÃO, O RESULTADO DE SEU RESTO POR 27 DEU 1?	
SIM	Esse número é o **inverso multiplicativo do determinante** da Matriz-chave e será usado para a **parte 3**. **Obs.:** Coloque ele no quadrado verde da **Parte 3**.
NÃO	A matriz informada não pode ser matriz-chave para a Cifra de Hill com 27 caracteres. Volte para a primeira planilha e verifique que ela não é invertível.

Imagem 5.6. Parte II do processo.

PARTE 3 - A MATRIZ DE DECODIFICAÇÃO			
ADJUNTA DA MATRIZ-CHAVE :	6	-11	MATRIZ ADJUNTA $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longrightarrow \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$
	-1	13	
iNVERSO MULTIPLICATIVO DA MATRIZ-CHAVE :	25		Deve ser obtido na tabela da **Parte 2**.
INVERSA :	150	-275	É a Matriz Adjunta multiplicada pelo Inverso Multiplicativo do determinante da Matriz-chave.
	-25	325	
MATRIZ DE DECODIFICAÇÃO :	15	22	É a Matriz Inversa considerando-se os restos da divisão de suas entradas por 27.
	2	1	

Imagem 5.7. Parte III do processo.

Assim, com o auxílio dessa matriz de decodificação e com a planilha de decodificação aplidada à mensagem do caça-palavras obteremos a tradução exposta na Imagem 5.8 a seguir.

MENSAGEM	M	X	N	Y	U	F	A	L	U	U	U	M	Y	C	B	J
DECODIFICADA	12	23	13	24	20	5	0	11	20	20	20	12	24	2	1	9

Imagem 5.8. Decodificação.

De fato, a palavra “UFAL” aparece nos blocos 3 e 4 da mensagem, no entanto, a decodificação não traduz-se em uma mensagem entendível e, portanto, essa não é uma solução para o caça-palavras criptografado.

5.2 Desafio: ès capaz?

DECIFRE-ME SE FOR CAPAZ
É CLARO QUE VOCÊ NÃO IRIA FICAR DE FORA DA BRINCADEIRA

Vamos ao exercício para ver se você pegou o jeito do quebra-cabeça, lembre-se: é importante achar uma mensagem que faça sentido. Observe o caça-palavras na Imagem 5.9 abaixo.

R	T	C	U
-	E	N	V
G	C	P	N
R	T	Z	W

Imagem 5.9. O seu desafio.

Aqui são válidas as mesmas considerações anteriores:

1. A mensagem foi codificada pela utilização da Cifra de Hill;
2. O alfabeto utilizado contém 27 caracteres, sendo os 26 primeiros as letras do alfabeto latino e o 27º o caractere Hífen (-);
3. A matriz chave utilizada é de ordem 2;
4. As entradas da matriz chave são números naturais menores ou iguais a 10;
5. Cada parte da mensagem está disponibilizada em uma linha da tabela;
6. Cada linha deve ser lida da esquerda para a direita.

Dessa vez, porém está escondido "-O-S", de forma que o bloco "-O" é o último de alguma linha e o bloco "-S" é o primeiro da linha seguinte.

Então Professor-leitor, tente inicialmente resolver o desafio proposto, vivenciando a experiência de decodificação antes de levá-la para a sala de aula. Essa etapa é importante para compreender as possíveis dificuldades dos estudantes e para explorar adaptações, como a criação de novos caça-palavras criptografados, ajustando o nível de complexidade conforme o contexto da turma.

5.3 Para além do "Decifre-me se for capaz"

Estamos chegando ao final deste manual, mas não ao fim das possibilidades de trabalho com a Cifra de Hill em sala de aula. Este capítulo teve como objetivo oferecer subsídio para que você, professor, explore a criptografia como uma ferramenta pedagógica capaz de articular conceitos matemáticos, investigação e resolução de problemas.

O desafio “Decifre-me se for capaz” representa apenas um ponto de partida. Ao vivenciar a experiência de decodificação, você é convidado a refletir sobre o potencial dessa abordagem e a adaptá-la às especificidades de suas turmas, seja por meio da criação de novos caça-palavras criptografados, da alteração das mensagens ou da escolha de diferentes matrizes-chave.

Espera-se, assim, que este material sirva como inspiração para práticas pedagógicas que promovam a participação ativa dos estudantes, valorizem o raciocínio lógico e favoreçam a construção significativa do conhecimento matemático, reconhecendo a criptografia como um campo fértil para a integração entre teoria, prática e criatividade.

Neste manual, além da versão para matriz-chave de ordem 2, deixei também acesso para as mesmas planilhas na versão da matriz-chave de ordem 3. Mas, por fim, quero deixar o convite para que, junto aos seus alunos, você possa também adaptar essas planilhas para outros objetivos, seja envolver matrizes de ordem maiores ou, até mesmo, utilizar alfabetos com uma variedade maior de caractéres.

Queremos que a Matemática deixe de ser apenas um conjunto de procedimentos e passa a ser um espaço de experimentação, diálogo e construção coletiva de sentidos. Vamos juntos nessa?

REFERÊNCIAS

- ARAÚJO, Ana Carolina Gonçalves. A Cifra de Hill sob o olhar das planilhas eletrônicas: o estudo de matrizes aplicado à criptografia por meio do Excel. 2026. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal de Alagoas. Maceió, 2026.

- INSTITUTO DE MATEMÁTICA PURA E APLICADA – IMPA. Retrospectiva 2024: 10 anos da medalha Fields de Artur Avila. IMPA – Instituto de Matemática Pura e Aplicada, 03 jan. 2025. Disponível em: https://impa.br/notices/retrospectiva-2024-10-anos-da-medalha-fields-de-artur-avila/. Acesso em: Dez/2025

- JEANRENAUD, Maria de Lourdes R. de A. A cifra de Hill. Temas e Conexões, ano I, n. 1, 2º semestre, 2013.

- LAUNAY, Mickaël. A fascinante história da matemática: da pré-história aos dias de hoje. Tradução de Clóvis Marques. Revisão da tradução de Anna Maria Sotero. 1. ed. Rio de Janeiro: Bertrand Brasil, 2019.

- MARTÍNS, Wellington de Sousa. Aplicação da álgebra moderna nos fundamentos da criptografia: cifras de César e cifras de Hill. 2016. Trabalho de Conclusão de Curso (Licenciatura em Matemática) – Universidade Federal do Tocantins, Campus Universitário de Araguaína, Araguaína, 2016.