A B A K Ó S
PUC Minas Instituto de Ciências Exatas e Informática

Criptografia e Livros Didáticos do Ensino Médio: Uma Análise Sobre as Novas Obras Didáticas Específicas do PNLD 2021*

Cryptography and High School Textbooks: an Analysis of the New 2021 PNLD Specific Didactic Works

Beatriz Fernanda Litoldo[1]
Douglas Ribeiro Guimarães[2]

Resumo

Neste artigo analisamos as novas obras didáticas específicas aprovadas pelo Programa Nacional do Livro e do Material Didático, edital de 2021, na frente de 'Ciências Humanas e Sociais Aplicadas em diálogo com a Matemática'. Para esta análise, nos aprofundamos na temática da Criptografia, visto que ela relaciona conceitos matemáticos com a interdisciplinaridade a partir de visões sociais e humanas, ou seja, é um tema que estaria de acordo com os princípios das obras citadas. De abordagem qualitativa, a pesquisa documental retratada no texto apresenta os resultados da investigação a partir das análises horizontal e vertical dos livros didáticos. Como discussões, apresentamos quatro categorias não disjuntas que emergiram dos dados: definições sobre criptografia; tipos de cifras, conceitos matemáticos e aplicações; tecnologias e entretenimento; e segurança da informação e interdisciplinaridade. Apontamos como principais resultados a pouca presença da Criptografia nas obras analisadas, sendo proeminente em apenas um livro dentre os nove investigados; a falta de articulação entre as áreas do conhecimento quando olhamos para a temática; e algumas incoerências conceituais e de aplicação da Criptografia. Refletimos que outros temas, conteúdos e discussões podem ser observados nessas obras, principalmente para trazer subsídios aos professores que farão uso delas a partir dos próximos anos.

Palavras-chave: Educação Matemática. Reforma do Ensino Médio. Criptografia. Livros didáticos. Cifras e códigos.

*Submetido em 18/07/2022 – Aceito em 13/09/2023

[1]Doutora em Ensino de Ciências e Matemática e Professora pela Universidade Federal do Triângulo Mineiro - UFTM, câmpus Uberaba/MG, Brasil– beatriz.litoldo@uftm.edu.br

[2]Doutorando em Educação Matemática, pelo Programa de Pós-graduação em Educação Matemática da Universidade Estadual Paulista - UNESP, câmpus Rio Claro/SP, Brasil. Professor do Centro Estadual de Educação Tecnológica Paula Souza, Brasil– douglas.guimaraes@unesp.br

Abstract

In this paper, we analyze the new specific didactic works approved by the Programa Nacional do Livro e do Material Didático, public notice of 2021, referring to the works of 'Applied Human and Social Sciences in dialogue with Mathematics'. For this analysis, we delve into the topic of Cryptography, since it relates mathematical concepts to interdisciplinarity from social and human perspectives, that is, it is a topic that would be in accordance with the principles of the didactic works cited. From a qualitative approach, the documental research portrayed in the text presents the results of the investigation from the horizontal and vertical analyses of the textbooks. As discussions, we present four non-disjoint categories that emerged from the data: definitions of cryptography; types of ciphers, mathematical concepts, and applications; technologies and entertainment; and information security and interdisciplinarity. We point out as main results little presence of Cryptography in the analyzed didactic works, being prominent in only one book among the nine investigated; the lack of articulation between the areas of knowledge when we look at the theme; and some conceptual and application inconsistencies of Cryptography. We reflect that other themes, contents, and discussions can be observed in these didactic works, mainly to bring subsidies to teachers who will use these materials in the coming years.

Keywords: Mathematics Education. High School reform. Cryptography. Textbooks. Ciphers and codes.

1 INTRODUÇÃO

Subsidiando as práticas pedagógicas dos professores e apresentando aos estudantes um modo de organização do conhecimento (científico), os Livros Didáticos (LD) são materiais importantes e estão fortemente presentes ao longo da formação do estudante, seja em sala de aula ou fora dela (MATIĆ, 2019). No caso das escolas públicas brasileiras, os LD representam uma peça central no currículo escolar, pois trazem, mesmo com algumas limitações, discussões curriculares apresentadas por meio de normativas e diretrizes para o conhecimento dos profissionais da educação (AZEVEDO, 2005; LAJOLO, 1996).

Diante da reforma do Ensino Médio, diversas mudanças nessa etapa escolar passaram a ocorrer no país, principalmente pela troca de carga horária, novos materiais didáticos, inclusão de partes diversificadas no currículo, entre outras. Ademais, a Base Nacional Comum Curricular – BNCC (BRASIL, 2018) também possui um papel fundamental na normatização de toda a Educação Básica, direcionando a constituição dos currículos estaduais e municipais, em particular, dos projetos políticos pedagógicos de cada escola brasileira.

Investigar como essas mudanças tem impactado a produção de novos materiais didáticos é o contexto da pesquisa que trazemos. Para isso, escolhemos aprofundar o olhar para a Criptografia, pois envolve conceitos matemáticos atrelados com discussões presentes em outras ciências. Desse modo, a delimitação de nosso estudo está relacionada com a compreensão da presença da Criptografia em LD aprovados no edital mais recente do Programa Nacional do Livro e do Material Didático (PNLD), na etapa do Ensino Médio.

No que segue, evidenciaremos a justificativa/pertinência de olhar para esses novos LD[3] e explicitaremos os motivos de analisar materiais que não são de Matemática, mas sim os que trazem essa área em diálogo com as Ciências Humanas e Sociais Aplicadas. Diante disso, nos questionamos: o que mostram os novos livros didáticos quanto ao tema Criptografia?

2 CRIPTOGRAFIA E EDUCAÇÃO MATEMÁTICA: UM ENTRELAÇAMENTO

Proveniente das palavras gregas *kriptós* (escondido, oculto) e *gráphein* (escrever), a palavra criptografia pode ser entendida como sendo uma maneira de escrever mensagens em cifras e/ou em códigos[4], com o objetivo de camuflar as mensagens a terceiros (TAMAROZZI, 2001). Desse modo, essa arte ou ciência possibilita que apenas a pessoa autorizada (destinatário) decifre e leia os conteúdos secretos. Historicamente, presente desde os tempos de guerra, a criptografia garantia (ou deveria garantir) a eficiência e o sigilo nas comunicações, considerados fundamentais para as estratégias de batalhas.

Conforme apontado por Singh (2008), a criptografia se desenvolveu a partir da necessidade, sempre presente, de proteção de dados, deixando para trás uma história permeada de conflitos entre os criadores de cifras e de códigos (criptógrafos) e os quebradores de cifras e de

[3]Estamos assumindo que os livros provenientes do PNLD aqui analisado são novos no que tange, por exemplo, às suas estruturas, aos modos de utilização e aos seus conteúdos abordados.

[4]Em síntese, a substituição de palavras/expressões é considerada um código, ao passo que a substituição de letras é definida como cifra (SINGH, 2008).

códigos (criptoanalistas). Esses conflitos ocorriam em meio às disputas de poder, sobretudo nas guerras. Nessa direção, o desenvolvimento de técnicas precisas de cifragem teve grande avanço depois do surgimento dos computadores modernos. A junção dessa tecnologia com as ideias de cifração/codificação e decifração/decodificação possibilitou a criação de cifras/códigos cada vez mais seguros e rápidos. A utilização de e-mail, redes sociais, operações online, transações bancárias etc. percorrem o campo da criptografia, fazendo uso dessa ciência como ferramenta de segurança de dados (SINGH, 2008).

Assim, temos hoje discussões frequentes sobre confidencialidades de informações ou de invasões a *sites* ou a documentos importantes, como por exemplo, os governamentais (talvez o caso mais famoso seja o das revelações do *Wikileaks*[5]). Desse modo, podemos dizer que esse tema vem ganhando os holofotes à medida que se integra com a sociedade e, consequentemente, com a população. Esse contexto de confiabilidade das informações já se fazia presente na literatura do século XX, com os contos de Sir Arthur Conan Doyle e de Edgar Allan Poe e, atualmente, o suspense e as tensões governamentais e o ciberespaço são temas presentes no campo do entretenimento, como em filmes e séries (LITOLDO, 2016).

Entretanto, a atenção dada à criptografia também se faz presente no meio científico. Muito se tem pesquisado sobre a criptografia e suas aplicações relativas às assinaturas e segurança das redes (CATALANO; PRISCO, 2018) e, particularmente, dessa temática na Matemática, à medida que se estuda conceitos matemáticos para o desenvolvimento de cifras e/ou códigos mais seguros e convenientes (SINGH, 2008). Todavia, ao lançar um olhar para esse tema na área da Educação Matemática observamos ainda uma tímida presença sobre esse entrelaçamento se comparado a outros focos de discussão.

Sobre essa possibilidade, compreendemos que a criptografia pode subsidiar a Educação Matemática como um elemento motivador e instigante para o estudo da Matemática (SANTOS, 2015) e propício para a promoção da interdisciplinaridade (BOMFIM, 2017; LITOLDO, 2016; OLGIN, 2011). Além disso, esse tema atua como um contexto da realidade para o desenvolvimento dos conhecimentos curriculares e suas inserções nas atividades humanas do dia a dia (OLGIN; GROENWALD, 2013; SINGH, 2008). Nessa perspectiva, e com o intuito de transportar a história da criptografia para dentro da sala de aula, é que atividades com o seu uso podem ser desenvolvidas e investigadas pelos estudantes com a exploração de conceitos previstos na Educação Básica.

Um dos primeiros trabalhos que aborda a criptografia no horizonte da Educação Básica, relacionado com o trabalho matemático, é o de Tamarozzi (2001). A proposta do autor se fundamenta na ação de cifrar e decifrar mensagens fazendo uso de matrizes invertíveis e função afim como chave cifradora e decifradora. Se, por um lado, demais estudos endossaram as considerações feitas por Tamarozzi (2001) relativos ao uso da criptografia para o trabalho com esses conteúdos (LITOLDO, 2016; OLGIN, 2011), por outro lado, existem investigações que ampliaram as possibilidades de utilização da criptografia. Por exemplo, encontram-se na literatura pesquisas que tratam da temática envolvendo os conceitos e/ou conteúdos de funções quadrá-

[5]Mais informações: <https://www.bbc.com/portuguese/noticias/2010/11/101129_wiki_ponto_ji>. Acesso em: 30 maio 2023.

ticas, exponenciais, logarítmicas e modulares (OLGIN, 2011) , além de análise combinatória, permutação, números primos, divisibilidade, construção de gráficos, polinômios, equações algébricas e curvas elípticas[6] (CARVALHO, 2016; VIDAL, 2019; LANA, 2016).

A partir de tais considerações estabelecemos reflexões sobre como a temática criptografia poderia chegar ao professor para além das propostas didáticas presentes nas pesquisas que entrelaçam esse tema e a Educação Matemática. Um dos caminhos que vislumbramos é pensar na sua inserção em materiais utilizados para a prática docente, como os LD. Compreendemos que nesses materiais poderia haver propostas fundadas na criptografia e que permitiriam a exploração dos conhecimentos curriculares, mais especificamente dos conceitos e/ou conteúdos matemáticos e a interdisciplinaridade desses com as demais áreas de conhecimento.

Todavia, olhar para essa possibilidade – Criptografia em LD – não é um ineditismo no âmbito da Educação Matemática, conforme mostraram Litoldo e Lazari (2014), mas consideramos relevante e pertinente investigar novamente esse entrelaçamento, pois novos LD estão chegando à sala de aula, devido às reformulações no PNLD.

3 OS NOVOS LIVROS DIDÁTICOS DIANTE DA REFORMA DO ENSINO MÉDIO

Por meio da Lei nº 13.415, mudanças na Lei de Diretrizes e Bases da Educação Nacional – LDB (BRASIL,) foram empregadas no âmbito do Ensino Médio. Entre as principais identificamos a ampliação da carga horária, a organização curricular frente ao que está definido na BNCC, a composição de parte diversificada do currículo (itinerários formativos), o estabelecimento de referências para as avaliações em larga escala, a formação integral e relacionada com o projeto de vida dos estudantes e a adequação dos currículos de formação dos professores com referência à BNCC.

Além dessas mudanças, a compreensão sobre o modo como a reforma foi estabelecida, partindo de uma Medida Provisória (nº 746, de 22 de setembro de 2016), já indicava receios no cenário educacional. Sobre isso, destaca-se que a reforma ocorreu em um período de tensões políticas e econômicas, com um tom de autoritarismo e imposição, no qual o objetivo foi "legitimar a hegemonia neoliberal no processo de disputa entre classes e frações de classes, em torno do projeto formativo e curricular do Ensino Médio" (SOUZA, 2021).

Ademais, Souza (2021) mostra como os setores empresariais são protagonistas dessas mudanças, pensando em seus interesses de produção atrelados com a formação dos estudantes. Além disso, na mesma direção que a BNCC (BRASIL, 2018) e as Diretrizes Curriculares Nacionais para o Ensino Médio (BRASIL, 2018b) pontuam, há um conjunto de dispositivos que visam normatizar a readequação dessa etapa escolar. Dentre eles, podemos mencionar a reelaboração dos currículos das redes de ensino, a adequação dos materiais didáticos, o controle da formação dos professores através de avaliações, entre outros.

Desse modo, ponderamos em adentrar na discussão sobre os materiais didáticos, especialmente os LD. O PNLD possui uma abrangência de avaliar e distribuir materiais para os

[6]Cabe ainda destacar que a Criptografia permite desenvolver um trabalho tanto na Educação Básica, quanto no Ensino Superior, conforme pode ser visto de forma mais específica nas pesquisas mencionadas.

estudantes das escolas públicas brasileiras (MAZZI, 2018). Ao longo das etapas da Educação Básica, editais específicos são publicados na intenção de que os autores e as respectivas editoras cadastrem suas obras para posterior avaliação e, em alguns casos, para a distribuição daquelas aprovadas. Especialmente por conta da reforma do Ensino Médio, diversas mudanças ocorreram nos editais dessa etapa, se comparar com anos anteriores.

Para o edital de convocação de obras didáticas para utilização nesse novo Ensino Médio (BRASIL, 2019a), por exemplo, cinco objetos foram definidos: Obras Didáticas de Projetos Integradores e de Projeto de Vida destinadas aos estudantes e professores (Objeto 1); Obras Didáticas por Áreas do Conhecimento e Obras Didáticas Específicas (ODE) destinadas aos estudantes e professores (Objeto 2); Obras de Formação Continuada destinadas aos professores e à equipe gestora das escolas públicas (Objeto 3); Recursos Digitais (Objeto 4); e Obras Literárias (Objeto 5). As informações sobre cada um dos objetos, bem como as adequações inerentes a eles estão disponíveis no edital 03/2019 (BRASIL, 2019a).

Nesta seção do texto, vamos nos restringir ao tratamento das obras do Objeto 2. O referido objeto trata de dois tipos de obras didáticas, primeiro, as que são destinadas às áreas do conhecimento, divididas em "Linguagens e suas Tecnologias", "Matemática e suas Tecnologias", "Ciências da Natureza e suas Tecnologias"e "Ciências Humanas e Sociais Aplicadas"; e segundo, as ODE, que são de "Língua Portuguesa", "Língua Inglesa"e "Ciências Humanas e Sociais Aplicadas em diálogo com a Matemática".

As obras por área do conhecimento são compostas por seis volumes que precisam abordar, todas as competências gerais, específicas e habilidades mencionadas na BNCC. Como consta no Guia[7] dessas obras, são possibilidades tidas pelos autores, abordar os conteúdos desses volumes em agrupamentos distintos, por exemplo, na área de Matemática, contemplar Probabilidade, Estatística e Matemática Financeira ou Geometria Analítica, Sistemas e Transformações Geométricas (BRASIL, 2021a).

Em relação as ODE, elas são compostas por volumes únicos. A obrigatoriedade é que o livro de Língua Portuguesa esteja vinculado, no momento de inscrição, com os materiais da área de Linguagens e suas Tecnologias. As outras duas obras específicas são independentes das coleções por área do conhecimento, ou seja, as editoras poderiam inscrever obras apenas específicas e/ou das áreas de conhecimento, sem inter-relações.

Vale dizer que quando se referem às obras didáticas, o edital está considerando o livro do estudante impresso, o material digital do estudante que é composto por uma coletânea de áudios (apenas as obras da área de Linguagens e suas Tecnologias e a específica de Língua Inglesa), o manual do professor impresso e o material digital do professor que contempla videotutorial (facultativo) e coletânea de áudios (BRASIL, 2019b).

Tomando atenção às obras concernentes à "Ciências Humanas e Sociais Aplicadas em diálogo com a Matemática" vimos que a proposta delas busca promover um diálogo entre as áreas de Ciências Humanas e Sociais Aplicadas e a de Matemática e suas Tecnologias, na pretensão de amparar as compreensões de ambas, bem como atribuir sentido a matemática ao bus-

[7] O Guia, conhecido oficialmente por 'Guia do Livro Didático', é um material elaborado pelos avaliadores dos livros, a partir da aprovação das obras, para subsidiar a escolha pelos professores.

car suas aplicabilidades nas situações e reflexões advindas dessas ciências (BRASIL, 2021b). Segundo o Guia dessas obras, elas objetivam efetivar a

> [...] interdisciplinaridade como um importante modo de promoção da produção de sentidos vinculados a ambas as áreas. Visa que essa produção se constitua por meio do próprio mundo que nos circunda. Ou seja, há fluxos que respeitam e compreendem que, nas últimas décadas, diversas transformações sociais, econômicas, políticas, culturais e tecnológicas têm impactado de forma significativa a vida das pessoas, as relações estabelecidas entre elas, o mundo do trabalho e, não poderia ser diferente, também o espaço da escola (BRASIL, 2021b, p. 20).

Além dessa configuração, é afirmado que esta obra "estimula a liberdade do pensar dos sujeitos [...] ao mesmo tempo em que valoriza o conhecimento científico e sua importância na atualidade" (BRASIL, 2021b, p. 20). Nessa direção, o Guia destaca a presença da contextualização e articulação dos saberes, compreendendo que estes se encontram atrelados à realidade, sendo expressos em propostas que envolvem "resolução de problemas, formulação de hipóteses e desenvolvimento de argumentação" (BRASIL, 2021b, p. 20).

Posto isso, dado esse conjunto de especificidades que constituem essa obra, é possível pensar em diversas temáticas que poderiam estar presentes no trabalho proposto por ela, dentre elas, destacamos a criptografia. Como mostra a literatura esse tema permite explorar o contexto das mensagens criptografadas, oportunizando a interdisciplinaridade da Matemática com as Ciências Humanas, por exemplo, ao tratar da história da criptografia e suas relações com a história da humanidade (SINGH, 2008), e ainda com as Ciências Sociais, ao tratar sobre a criptografia na Era da Informação, e como isso influencia a política e a economia, por exemplo, nas questões relacionadas ao poder, confiabilidade e liberdade (LITOLDO, 2016).

Ademais, as pesquisas que se debruçam relacionar a Criptografia e a Educação Matemática vêm evidenciando que tal tema oportuniza desenvolver com os estudantes momentos formativos instigantes, pautados na investigação e resolução de problemas, na qual possibilita ofertar processos de ensino e de aprendizagens fundados na autonomia, nas heurísticas e nos conhecimentos prévios para o desenvolvimento, tanto dos conhecimentos matemáticos quanto o de outras áreas (CARVALHO, 2016; OLGIN, 2011; VIDAL, 2019; LANA, 2016).

Diante do exposto, percebemos que as mudanças impactadas pela reforma do Ensino Médio, particularmente daquelas relacionadas com os novos LD, precisam de reflexões e investigações no sentido de contribuir com a literatura, principalmente para auxiliar o trabalho pedagógico do professor ao fazer uso desses materiais.

4 METODOLOGIA

As análises aqui apresentadas são frutos de um estudo que teve como objetivo investigar a presença do tema Criptografia em LD aprovados pelo PNLD 2021. Sendo orientada por uma metodologia qualitativa (GOLDENBERG, 2011) associada a uma pesquisa documental (LÜDKE; ANDRÉ, 1986), o presente texto toma atenção em apresentar e discutir quantas e quais obras tratam dessa temática, de que forma ela é abordada, quais conceitos matemáticos

são discutidos e se a proposta de discussão com esse tema está posto na interdisciplinaridade e como ela se dá – implícita e/ou explicitamente. Para este texto, em virtude da limitação de páginas e da demanda de dados, iremos focar as análises apenas sobre a parte conceitual do livro, isso é, as tarefas presentificadas nas seções que tratam da criptografia será foco de análise em posterior artigo.

Os LD selecionados para esse estudo foram aqueles oriundos do PNLD 2021 relativas às ODE de "Ciências Humanas e Sociais Aplicadas em diálogo com a Matemática". Essas obras devem ser trabalhadas durante todo o Ensino Médio. A opção por esses livros deu-se pelo fato da temática criptografia permitir trabalhar conceitos e/ou conteúdos de modo interdisciplinar. Como a proposta das obras específicas é justamente tratar das áreas de conhecimento numa perspectiva interdisciplinar acreditamos que seriam nesses livros que a temática poderia ser tratada e melhor explorada. Do total de 10 livros aprovados no PNLD 2021, foi possível ter acesso a nove deles. Desse modo, as nove obras foram analisadas quanto à presença da criptografia em seus conteúdos.

Seguindo a estrutura de análise horizontal e vertical proposta por Charalambous *et al.* (2010) a análise dos dados seguiu as seguintes etapas metodológicas. Na análise horizontal realizamos uma identificação nas obras quanto a suas autorias. Na sequência, efetuamos uma busca pela temática criptografia fazendo uso das palavras-chave: criptografia, cifras e códigos. Essa etapa evidenciou que em cinco LD a Criptografia é, ao menos, citada e, ao dar continuidade, buscamos especificar a localização do tema nos materiais.

Tendo situado então as localidades onde o tema da criptografia era abordado nas obras, deu-se início a análise vertical por meio de uma leitura na íntegra do conteúdo disposto no livro quanto a suas partes conceituais. Simultaneamente a essa leitura, as passagens do conteúdo de interesse desta investigação foram sendo selecionadas e arquivadas para posterior aprofundamento na análise. Ao final deste processo, foi possível identificar que, das cinco obras resultantes da primeira triagem, apenas duas delas abordavam a temática de modo significativo, sendo que as demais (três) traziam apenas menções ou pequenos trechos sobre.

Desse modo, os dados que constituem esse estudo provieram de dois LD, a saber, Dimensões (SELKE *et al.*, 2020) e Moderna Plus (PAIVA *et al.*, 2020). Doravante, iremos nos referir a essas duas obras como L_1 e L_2, respectivamente. Por fim, os dados advindos da análise vertical foram analisados de modo qualitativo, à luz dos aportes teóricos dialogados com a criptografia, buscando, sempre como propósito final, alcançar os objetivos postos nesta investigação. Assim, neste processo surgiram quatro categorias de análise não disjuntas, a saber, definições sobre criptografia; tipos de cifras, conceitos matemáticos e aplicações; tecnologias e entretenimento; e segurança da informação e interdisciplinaridade[8].

[8]Cabe ressaltar que os dados fazem parte, em sua maioria das vezes, em mais de uma categoria, todavia a opção por separá-los foi tomada de modo que seria mais organizado dar o enfoque de discussão de acordo com a categoria correspondente.

5 DESCRIÇÃO E ANÁLISE DOS DADOS

Conforme as orientações para o professor nas duas obras analisadas, a proposta do livro é mostrar um diálogo com as duas áreas do conhecimento, de modo que relações com o cotidiano dos estudantes possam ser estabelecidas. Na perspectiva dos Temas Contemporâneos Transversais (BRASIL, 2019b), que compõem documentos auxiliares à BNCC (BRASIL, 2018), as obras abarcam Multiculturalismo, Ciência e Tecnologia, Cidadania e Civismo, Economia, Saúde e Meio Ambiente.

Essa proposta ainda encontra amparo nas metodologias ativas para o caso da obra L_1, como aprendizagem baseada em projetos, sala de aula invertida e aprendizagem baseada em problemas. Ou seja, preconizam autonomia e protagonismo para os estudantes, em suas construções do conhecimento. No caso do livro L_2, o pensamento científico, o pensamento computacional, as práticas de pesquisa e o uso de tecnologias digitais são outras estratégias usadas para compor o diálogo com as áreas do conhecimento da obra didática.

Ambos os livros são organizados em oito capítulos, sendo que a divisão do livro L_1 é feita, primeiro, em quatro unidades e, cada uma delas possui dois capítulos. A presença da criptografia em L_2, por exemplo, ocorre no último capítulo do livro, sendo que a discussão toda é voltada para essa temática. Já em L_1, a criptografia faz parte de uma seção do capítulo "Conexões digitais", presente na unidade "Cidadania". Observamos que essa diferença no tratamento da temática, não apenas quantitativa (quantidade de páginas de cada uma), mas qualitativamente, foi percebida ao longo da análise.

No caso de L_2, por exemplo, as orientações para o professor já indicam a relevância, a atualidade, o interesse e a aplicação da Matemática no dia a dia como meios para justificar a inclusão de um capítulo inteiro sobre criptografia. Esses meios mostram a importância dessa temática por estar atrelada com a proteção dos dados, principalmente pelo impacto dos computadores e da internet, além de ser uma discussão que instiga os estudantes por meio de brincadeiras e da riqueza com que os conceitos matemáticos subjacentes à criptografia acabam por garantir a segurança na troca de mensagens.

Nessa mesma obra é indicado que o desenvolvimento do capítulo sobre criptografia seja feito a partir das interações dos professores de Matemática e História. Ao primeiro caberia comentar sobre os conteúdos de matrizes e bases binárias, já ao professor de História, os comentários em relação ao imperador Júlio César, os eventos históricos e as guerras, que são pontos que permeiam o capítulo.

5.1 Definição sobre criptografia

Em ambas as obras a definição sobre a criptografia é mencionada. Tal referência é feita logo no início da seção, como é o caso em L_1 ou do capítulo, como feito em L_2. A nosso ver, essa abordagem se faz pertinente ao passo que apresenta aos estudantes primeiramente o significado do termo e, de forma consequente, sua serventia/utilização.

Assim, abordando a definição por meio da etimologia da palavra criptografia, em L_1 (p.

76) ela é colocada de forma breve da seguinte forma: "A palavra é derivada do grego *kriptos* (secreto) e *grafia* (escrita) e reúne um conjunto de técnicas de envio e recepção de informação de maneira segura". Já em L_2 essa abordagem etimológica não acontece, entretanto, a obra faz menção a sua definição em mais de um momento logo na introdução de seu capítulo. De início ela apresenta o seguinte trecho de modo a exemplificar o que seria uma chave de escrita cifrada:

> Suponha que você e um amigo querem trocar mensagens escritas de modo que mais ninguém consiga compreendê-las. Para isso, vocês podem combinar um código com o qual o emissor codifique a mensagem e o receptor a decodifique. Esse código é chamado de chave da escrita cifrada (L_2, 2020, p. 113).

Na sequência, a obra traz uma definição mais ampla, na qual considera de forma explicita a criptografia enquanto uma ciência da comunicação secreta, em que as técnicas e os princípios são utilizados para codificar/decodificar mensagens. Em seguida, volta-se a tratar de sua definição, reforçando que "criptografar uma mensagem significa torná-la ininteligível a quem não conhece o código. Esse código é chamado chave criptográfica ou senha. Apenas quem conhece a chave tem acesso à forma inteligível da mensagem"(L_2, 2020, p. 113). Além disso, é somente nessa obra que o termo criptoanálise é mencionado e, mais que isso, definido, sendo esse último colocado como o "estudo das técnicas de decodificação de mensagens cifradas, sem o conhecimento prévio da chave que as gerou"(L_2, 2020, p. 113).

Assim sendo, compreendemos que as definições trazidas nas duas obras são pertinentes para iniciar os estudos com a criptografia. Mesmo que em L_2 não há indicação da etimologia da palavra, mais significados são abordados sobre essa ciência ao longo do capítulo, contribuindo com outros elementos relativos à sua definição. No caso de L_1, é interessante a explicitação do termo, contudo, ela ocorre de maneira sintética e pouco aprofundada, o que pode estar relacionado com a presença da criptografia em apenas uma seção do livro, ou seja, enquanto parte de um capítulo todo, o que difere da obra anterior.

5.2 Tipos de cifras, conceitos matemáticos e aplicações

Diante das distintas possibilidades de métodos para a cifragem de uma mensagem, as obras apresentam exemplos de cifras que vão desde as mais simples, como o uso de símbolos, até as mais complexas, como o sistema RSA. Em L_1, na seção "Criptografia digital", como o próprio título sugere, menciona sobre alguns tipos de cifras que estão ligadas ao ciberespaço. Nesse cenário, se faz necessário o uso de cifras poderosas[8] que tornem a comunicação via rede cada vez mais segura. Assim, como referências de cifras que surgem e são utilizadas na era digital é citada o *American Standard Code for Information Interchange* – ASCII, o qual associa cada algarismo ou letra a um número binário que possui sete dígitos. Essa cifra, como aludido pelos autores, é considerada uma chave simétrica, uma vez que os algoritmos de codificação e decodificação são equivalentes. Além desse, de forma a exemplificar um tipo de cifração que se fundamenta na chave assimétrica, isso é, aquela que se utiliza de chaves públicas e privadas

[8] A noção de cifra poderosa diz respeito a qualidade de uma cifra em ser 'quebrada' facilmente. Quanto mais difícil descobrir a cifra, mais poderosa ela é.

(que são distintas), os autores citam sobre o sistema RSA. De forma breve, o seguinte relato sobre essa cifra é apresentado ao estudante:

> O algoritmo de assinatura digital RSA (Rivest-Shavir-Adleman) foi desenvolvido em 1977 pelo matemático estadunidense Ronald Rivest (1947), pelo criptógrafo israelita Adi Shamir (1952-) e pelo informático e biólogo molecular Leonard Adleman (1945-), no Massachusetts Institute of Technology (MIT). Esse algoritmo utiliza duas chaves, uma de codificação (chave pública) e outra de decodificação (chave privada, a qual apenas o destinatário da informação possui). [...] O algoritmo RSA codifica apenas números; por isso, usa o sistema ASCII para codificar. Para que os cálculos fiquem mais evidentes, é preciso associar cada letra do alfabeto a um número, conforme o quadro a seguir:
>
> | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
> |---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
> | 1 | 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 |
>
> L_1, 2020, p77.

Os autores sugerem aos professores que reforcem para os estudantes a relevância da criptografia no contexto atual, em que as informações sobre cada um de nós estão presentes na internet e que a proteção dos dados é fundamental para evitar o uso prejudicial dos mesmos. Além disso, orientam os professores para questionar os estudantes em relação à como protegem seus dados e quais ações costumam usar para essa proteção no cotidiano. Como sugestão de ampliação do conteúdo, indicam o acesso à tabela ASCII pelos estudantes, para que possam criptografar mensagens a partir dos números binários.

Diferentemente, o livro L_2 não faz menção aos termos "cifras simétricas"e "cifras assimétricas", embora traga em seu conteúdo exemplos de seus tipos. Antes mesmo do capítulo destinado a apresentação e discussão sobre a criptografia (Capítulo 8, p. 113 – 127) os autores mencionam a cifra ASCII no Capítulo 5, destinado aos "Sistemas digitais e a base binária". Após discorrer sobre o significado e aplicação dos *bits* e *bytes*, os autores apresentam uma seção intitulada "*Bytes* e o padrão ASCII"e uma subseção "Tabela ASCII padrão", no qual tem como foco esclarecer sobre o sistema padrão de caracteres ASCII.

Já no capítulo destinado ao trato com a criptografia, certos tipos de cifras são exemplificados, alguns por meio de seus nomes conhecidos, como a Cifra de César e a Cifra de Hill, outros apenas pela menção de sua definição/algoritmo de cifração. Desse modo, como forma de introduzir o tema, os autores de L_2 reportam uma situação fictícia em que os estudantes poderiam trocar mensagens cifradas a partir da substituição das letras do alfabeto por números, na ordem em que aparecem (e.g., 1 representa a letra 'A', 2 a letra 'B' etc.).

Nesse exemplo, o processo de cifração se embasa apenas em associar cada número natural a uma letra do alfabeto e realizar a substituição das letras da mensagem pelos seus números correspondentes. Utilizando dessa mesma ideia, na seção "A criptografia como tática de guerra" é apresentada a Cifra de César, a qual assim ficou conhecida por ser um tipo de cifra muito utilizada pelo imperador romano Júlio César (100 a.C. – 44 a.C.). Em linhas gerais, podemos dizer que essa cifra se utiliza do método de descolamento do alfabeto, em que a subs-

tituição das letras ‘A’, ‘B’, ‘C’ da mensagem refere-se à ‘D’, ‘E’, ‘F’, respectivamente, ou seja, o alfabeto se deslocaria três casas na contagem das letras[10].

A construção dessa cifra é apresentada nas orientações para o professor por meio de um passo a passo, em que são utilizadas folhas de cartolina e marcações com régua e lápis, confeccionando uma "régua"deslizante. O objetivo dessa construção, na visão dos autores, é de auxiliar o processo de codificação/decodificação dos estudantes por meio da régua criada, simplificando o processo e contribuindo com exemplos de aplicação da cifra. Outro exemplo sugerido para o trabalho pedagógico está focado nas cifras de transposição, em que não há substituição de letras como na Cifra de César, mas sim uma reorganização. Os autores trazem duas situações diferentes e, por meio de tabelas, indicam para o professor como o processo pode ser feito, abordando mais significados para os conceitos apresentados aos estudantes.

Ambas as cifras acima podem ser consideradas criptografias simples (SINGH, 2008), pois são cifras simétricas e não estão associadas de forma direta com conceitos matemáticos. Todavia, embora a Cifra de Hill também seja uma cifra simétrica, a consideramos mais elaborada que a de César, pois ela está diretamente fundamentada em conceitos matemáticos. Essa cifra, por sua vez, é tratada pelos autores de forma mais detalhada conjuntamente com seu conteúdo matemático, o qual será abordado mais adiante ainda nesta seção.

Os autores mencionam que esta cifra foi criada em 1929, por um matemático estadunidense chamado Lester S. Hill (1891-1961), explicando que esse tipo de cifra “envolve múltiplos conceitos de Álgebra Linear, porém estudaremos uma variação simplificada, que necessita apenas de algumas noções elementares sobre matrizes” (L_2, 2020, p. 119). Após detalhar os processos de utilização nesse tipo de cifra, exemplificando a cifração e decifração da frase BOA SORTE, os autores encerram essa seção argumentando que tais procedimentos são tidos como simples e que para outras situações que envolvam segurança nacional, como por exemplo, realização de movimentações financeiras em bancos e/ou operações comerciais via internet, os métodos de cifração e decifração são extremamente complexos (L_2, 2020).

Assim, nesta direção, os autores trazem, de forma muito simplista, o exemplo da criptografia que se utiliza de número primos. Embora eles não mencionem que tipo de criptografia é essa (por exemplo, o sistema RSA faz uso dos números primos), os autores explanam sobre como é interessante a utilização desses números para a cifração de informações, pois esse tipo de cifra é considerado como uma criptografia poderosa, visto que a fatoração em números primos não é algo trivial.

Permeando as apresentações e discussões sobre o tema criptografia, especificamente, sobre os tipos de cifras, existem alguns conceitos matemáticos que são abordados nas obras. Em L_1, de forma breve e concisa aparecem os conceitos de linguagem binária, algoritmo e números primos em caixas de destaque, à qual é chamada pelo livro como "Boxe-conceito". Segundo a obra, esse boxe compreende explicações de palavras ou expressões ressaltadas no corpo do texto em negrito e traçado vermelho que objetivam subsidiar a compreensão dos conceitos principais abordados, por meio de esclarecimentos de conceitos adicionais.

[10]Para mais informações a respeito das cifras de cifra de César ver Singh (2008).

O conceito de linguagem binária é tratado logo no início do capítulo sendo envolto pela discussão sobre o surgimento da internet. O foco é apresentar ao estudante que a linguagem binária é o modo pelo qual um semicondutor estabelece uma comunicação entre todos os componentes eletrônicos que constituem um computador. Nesse momento os autores ainda não mencionam nada sobre o tema criptografia. Todavia, mais à frente, na seção destinada à sua discussão, os autores resgatam o conceito da linguagem binária para discutir sobre a criptografia digital e de como o código binário se faz importante para a linguagem computacional. Como exemplo desse tipo de linguagem, os autores citam a cifra ASCII.

Em L_2 há uma seção intitulada "A Matemática e a Estatística aplicadas à criptografia"na qual se inicia argumentando que a criptografia está bastante próxima dessas duas áreas por meio dos conteúdos de números primos, matrizes, congruência numérica, distribuição de frequências e análise combinatória. Como forma de exemplificar essa relação, os autores apresentam alguns tipos de cifras, os quais se encontram fundamentados em determinados conceitos e conteúdos matemáticos. Assim, para a Cifra de Hill, a obra traz o conteúdo de matrizes abordando o conceito, a multiplicação e a inversão de matrizes. Esses conceitos são considerados como pré-requisitos para compreender o método dessa cifra. Após a obra apresentar de forma resumida cada um deles, um exemplo é dado como forma de aplicação.

A definição dos números primos é mencionada, sendo sua utilização atrelada a chaves para cifrar as mensagens. Nesse método, quanto maior for o número primo utilizado mais seguro estará a mensagem, pois números primos grandes dificultam a decifragem da mensagem para aqueles que não conhecem a chave. Isso está relacionado à dificuldade em fatorar a chave cifradora, que é o resultado da multiplicação de dois números primos grandes.

O conceito de distribuição de frequências de letras está vinculado ao método de criptoanálise (procedimentos de decifração da mensagem sem a chave cifradora), em que o texto ou mensagem é cifrado por meio de símbolos, no qual cada letra do alfabeto é associada a um símbolo diferente. Para um texto escrito em certo idioma, deter um conhecimento anterior sobre a frequência relativa das letras que formam palavras do idioma pode contribuir para a identificação da letra associada a cada símbolo usado na mensagem cifrada (L_2, 2020).

Na continuidade, os autores apresentam informações relativas às frequências de letras na língua portuguesa. Nesse caso, a letra ‘a’, por exemplo, é a letra mais frequente e pode assim corresponder ao símbolo que mais aparece em um texto cifrado neste idioma, seguida pelas letras ‘e’, ‘o’ e ‘s’. Um detalhe importante é que para obter sucesso nesse método de decifração, é necessário que o texto cifrado seja relativamente longo, de modo a permitir que as frequências de suas letras e/ou símbolos sejam significativas.

Como forma de fechar essa seção, a obra apresenta uma situação, supondo que se tem um texto escrito em português, com 3.600 letras, no qual sua cifração está embasada em simbologias. Partindo de uma palavra formada por símbolos e realizando a contagem de suas aparições no texto (frequência absoluta), são apresentados ao estudante os cálculos alusivos às suas frequências relativas. Por fim, as comparações entre as frequências relativas das letras da língua portuguesa com as simbologias no texto são mencionadas, chegando-se à conclusão à qual letra

o símbolo está associado e, concluindo então, a decifração da palavra.

As aplicações da criptografia, principalmente nos dias de hoje são referidas pelas duas obras, todavia, em L_1 isto é feito de forma singela, apenas com a citação de sua utilização em contextos de segurança digital, como de troca de mensagens por celular e transações financeiras. Já em L_2 a explanação de suas aplicações é tomada de forma mais detalhada em uma seção do capítulo chamada "A criptografia no domínio público". Aqui, os autores mencionam o fato de que a cada dia as mensagens cifradas têm ganhado importância no cotidiano das pessoas, afirmando que estamos "tão habituados à presença da criptografia em nossas vidas que, às vezes, nem a percebemos" (L_2, 2020, p. 115). Como exemplos do uso da criptografia no cotidiano são citados as seguintes situações:

> - Senha bancária: sequência de caracteres que funciona como uma chave que abre a porta de acesso a uma conta em banco. Ao digitar a senha em um canal de atendimento, um sistema de segurança a criptografa de modo que algum eventual invasor (*hacker*) não consiga descriptografá-la.
> - Compras pela internet: ao preencher formulários com os dados pessoais e do cartão de crédito em um **site confiável**, alguns recursos de segurança permitem que os dados sejam transmitidos por uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente, por meio de certificados digitais.
> - Arquivos confidenciais: informações sigilosas podem ser armazenadas digitalmente em arquivos protegidos por senhas criptografadas. Algumas empresas, além das senhas, criptografam o conteúdo do arquivo. (L_2, 2020, p. 115, grifo dos autores).

Além de suas aplicabilidades na atualidade, em ambas as obras é dissertado sobre o uso da criptografia ao longo dos anos, principalmente durante a Segunda Guerra Mundial. O aperfeiçoamento dos tipos de cifras para uma criptografia mais poderosa esteve muito ligado a esfera militar, em que trocar mensagens em sigilo poderia influenciar de forma decisiva no curso de ataques e/ou defesas de nações. Essa importância da criptografia na história das guerras é destacada na obra L_2 quando, por exemplo, faz a menção do feito de Alan Mathison Turing (1912-1954) e seu reconhecimento por parte dos ingleses. Alan Turing, como mais conhecido, construiu uma máquina que foi capaz de decifrar os códigos nazistas e esse feito de acordo com alguns historiadores "antecipou o fim da guerra em pelo menos dois anos, poupando milhares de vidas" (L_2, 2020, p. 115). A importância de Alan Turing na evolução da criptografia e, consequentemente, na história da humanidade reverberou no reconhecimento dos ingleses ao escolherem ele, por meio de uma votação popular, como sendo o britânico estampado na cédula de 50 libras.

Diante dessas discussões sobre os tipos de cifras, os conceitos matemáticos presentes e as aplicações desenvolvidas a partir da temática Criptografia, compreendemos que é notória a limitação da obra L_1 ao abordar essas discussões. Um ponto que diferencia as duas obras, visto que apresentaram ideias semelhantes, está no uso do código ACSII, em que os autores de L_2 incluem a tabela que relaciona os números binários com os algarismos e letras no que é apresentado aos estudantes, mas em L_1 ela é limitada a apenas um *link* disponível nas orientações para

o professor. Observamos que, caso o professor esteja apenas com a obra física, dificilmente teria acesso ao *link*, devido ao enorme uso de caracteres e símbolos.

5.3 Tecnologias e entretenimento

A presença da tecnologia ao abordar o tema Criptografia foi mencionada nos dois LD analisados. Atrelada à sua história na corrida da cifração/codificação e decifração/decodificação de mensagens, as tecnologias se fizeram presentes na evolução das cifras/códigos e algumas destas foram abordadas pelos autores, como o bastão de Licurgo (ou cítala), a Colossus e, a mais conhecida, já presente em filmes e séries, a Enigma.

O bastão de Licurgo tem como base a criptografia de transposição, isso significa que as letras do alfabeto são somente rearranjadas, estabelecendo um anagrama. Essa ferramenta, datada do século V a.C., é considerada a primeira tecnologia criptográfica militar, muito utilizada pelos espartanos, em que se constituía apenas por um bastão de madeira e uma tira de couro ou papiro, a qual era espiralada (SINGH, 2008). A máquina Colossus, inventada pelos britânicos, chegou a Bletchley no fim de 1943 e era composta por 1.500 válvulas elétricas. Ela era uma máquina totalmente programável e foi considerada por alguns pesquisadores como sendo a precursora do computador digital (SINGH, 2008). Historicamente, a Colossus foi desenvolvida para combater uma cifra utilizada na comunicação entre Hitler e seus generais, durante a Segunda Guerra Mundial.

Já a máquina Enigma pode ser tida como uma versão elétrica do disco de cifras de Alberti[11], mas, muito mais complexa. Segundo Singh (2008, p. 146) a Enigma "se tornaria o mais terrível sistema de cifragem da história" da criptografia. Patenteada por Scherbius, seu inventor, em 1918, a máquina de cifragem vinha dentro de uma caixa compacta, tendo como dimensões 34x28x15 cm e pesando, aproximadamente, 12 quilos. Singh (2008, p. 161) afirma que essa máquina "deu aos alemães o sistema mais seguro de criptografia do mundo".

Exprimidas no início do tratamento da temática, nas três situações elas encontram-se atreladas ao caráter histórico. O bastão de Licurgo é apresentado na seção "A criptografia como tática de guerra" fazendo referência a sua utilização pelos espartanos e exemplificando o seu modo operante (L_2, 2020). A máquina Colossus é abordada na seção nomeada "Pós-Segunda Guerra Mundial: o desenvolvimento dos computadores no mundo" (L_1, 2020) e como o próprio nome sugere, a menção sobre ela encontra-se vinculada ao contexto do desenvolvimento dos computadores depois da Segunda Guerra Mundial. De todas as citações sobre as tecnologias da criptografia, essa é a única que não foi explorada na parte conceitual dos livros, estando posta na obra apenas pela sua imagem e descrição, sendo mencionada novamente mais à frente ao tratar da Enigma, fazendo referência à criptografia mecânica.

Já a Enigma aparece em ambas as obras estando ela relacionada à parte histórica da Segunda Guerra Mundial. Todavia, no livro L_1 ela é brevemente mencionada na seção nomeada

[11] No ano de 1440 Leon B. Alberti inventou um mecanismo de criptografia por transposição que se constituía por dois discos de cobre de tamanhos diferentes. Desse modo, era gravado na borda dos discos o alfabeto e ambos eram fixados por um pino, que exercia o papel de eixo. Os discos podiam ser girados de forma independente, configurando associações diversas entre os alfabetos das bordas.

"Criptografia", dentro do capítulo 4 "Conexões Digitais". Já no livro L_2 o contexto do surgimento dessa máquina e sobre ela (sua composição e funcionalidade) é mais explorada na seção destinada a "Texto Complementar", na dissertativa sobre "Poloneses foram os primeiros a decifrar o código Enigma", citando nomes muito importantes no contexto histórico da criptografia concernente à Enigma, como o caso de Alan Turing, Hans-Thilo Schmidt e Marian Rejewski. Essa seção encontra-se no final do capítulo e para o seu encerramento, na caixa nomeada "Sugestões", os autores da obra indicam um vídeo que explora mais informações sobre a máquina.

Essas três tecnologias mencionadas pelas obras, segundo L_1 podem ser classificadas em tecnologias de criptografias manuais, mecânicas e digitais. Compreendemos que, enquanto a primeira faz uso essencialmente de lápis e papel (e.g., Licurgo), e a segunda utiliza máquinas para o processo de cifração/codificação e decifração/decodificação (e.g, Colossus e Enigma), a terceira, embora também se tome uso de máquinas, aqui, elas são computadores extremamente eficientes ligados a redes no ciberespaço. Nos dias de hoje, nos encontramos na era da criptografia digital, haja vista o avanço da tecnologia e o desenvolvimento de computadores cada vez mais rápidos.

Ao buscar nas obras menções concernentes ao entretenimento, encontramos a referência sobre o filme "O jogo da imitação" nos dois livros investigados em caixas como "Fica a dica" em L_1 e "Sugestões" em L_2. O filme retrata a história de Alan Turing e sua equipe na busca da decifração da máquina Enigma. Além dessas, em L_2 é possível encontrar referências a outros vídeos sobre criptografia e sua presença atualmente e, também, outros vídeos com temática sobre o sistema binário e a funcionalidade da Enigma.

Diante desses achados, foi possível observar que, embora existam momentos em que filmes e vídeos são sugestionados nos livros, não há uma exploração pedagógica sobre eles, nem mesmo nas orientações ao professor tal ação é mencionada. Entendendo que a literatura e, posteriormente, os filmes e séries encontram-se muito entrelaçados à história da criptografia e a suas contextualizações nos dias atuais, compreendemos que essas fontes permitem desenvolver uma pluralidade de discussões e tarefas acerca da temática, inclusive numa perspectiva da interdisciplinaridade aliada a reflexões críticas sobre a matemática e seu papel na criptografia. Além disso, também entendemos que fazer uso da literatura e/ou de filmes e séries contribui para motivar e instigar os estudantes no estudo do conteúdo proposto, visto que para muitos, essas fontes são próximas de seus cotidianos.

5.4 Segurança da informação e interdisciplinaridade

Assegurar sigilo entre troca de mensagens está intrinsecamente ligado a própria definição da criptografia, a qual por consequência, está relacionada com contextos históricos e avanços tecnológicos da humanidade. Nesse sentido, não tem como abordar e discutir criptografia sem situar suas evoluções e utilizações na história das guerras, por exemplo, e nem ao menos citar sobre o universo do ciberespaço no âmbito da segurança de dados.

Posto isto, foi possível observar que em ambas as obras os contextos históricos pelo qual a criptografia estava e vem sendo inserida foram mencionados. Em L_1 na seção "O surgimento

da internet" os autores citam sobre a criação da internet no período da Guerra Fria. De forma a trazer o contexto pelo qual a segurança da informação estava ligada a esse momento histórico os autores fazem uma explanação sobre o ocorrido na época, situando o conflito entre Estados Unidos e União Soviética, tendo como exemplo a Crise dos Mísseis em 1962. Segundo os autores, os militares estadunidenses consideravam a importância de comunicações seguras, diante de possíveis ataques nucleares.

Na sequência do capítulo existe uma apresentação e discussão sobre internet e a globalização, incluindo aqui aquelas relacionadas às exposições nas redes sociais e as *fake news*. Na seção mais a frente que tem como foco tratar especificamente da criptografia, os autores fazem menção as *fake news* e aos dados manipulados, chamando atenção para o cuidado que se deve ter ao trocar informações no meio digital. Explicam que a segurança das comunicações é uma preocupação antiga, principalmente pelo contexto da Segunda Guerra Mundial e da dependência de mensagens sigilosas. Concluem que, "com o desenvolvimento digital das últimas décadas, a velocidade das informações aumentou, e a garantia de sigilo tornou-se cada vez mais necessária, de maneira que a criptografia passou a ser essencial na segurança digital" (L_1, 2020, p. 76).

Em L_2 na introdução do capítulo que trata da criptografia já se tem uma contextualização histórica evidenciando que ela é tão antiga como a importância de manter em segredo a comunicação escrita. De forma a evidenciar essa afirmação, os autores de L_2 mencionam sobre a existência de "registros dessa prática em hieróglifos egípcios, datados de 1900 a.C., contando que os escribas dos faraós substituíam trechos e palavras em documentos por símbolos enigmáticos, que dificultavam o entendimento por parte de pessoas alheias aos interesses do império" (L_2, 2020, p. 113).

Após essa explanação, a primeira seção desse capítulo trata do contexto militar, apresentando a Cifra de César e explanando sobre seu uso pelo imperador romano Júlio César. Além dela, os autores fazem menção que a prática de se criptografar mensagens como tática militar já teria sido utilizada nas guerras espartanas datadas dos séculos V a.C. e IV a.C. por meio do bastão de Licurgo. Na continuação histórica, é citado que sua utilização foi marcante durante a Segunda Guerra Mundial, trazendo em destaque os feitos de Alan Turing para com a decifração e, consequentemente, para a contribuição dele com o fim da guerra.

Destinando uma seção específica para tratar com mais detalhes sobre o enlace da história com a evolução da criptografia, em "Texto Complementar", tem-se uma dissertativa chamada "Poloneses foram os primeiros a decifrar o código Enigma". Aqui é mencionado, por exemplo, sobre a Enigma ter sido uma das mais poderosas armas da Alemanha nazista, mesmo antes e ao longo da Segunda Guerra Mundial. Na sequência desse narrar histórico, os autores discorrem sobre a espionagem polonesa para com a interceptação das mensagens alemãs, contando como a Enigma e sua decifração influenciou nos rumos desse conflito.

Notamos que nessa obra os autores trouxeram as discussões sobre a segurança de informações e o contexto histórico de forma pouco entrelaçada. Em uma seção separada, intitulada "Explorando conexões", o texto "Remotabilidade e segurança da informação na era do traba-

lho a distância" aborda sobre os impactos da tecnologia no mundo profissional, bem como nas ferramentas de trabalho, por exemplo, o e-mail substituindo as diversas caixas de arquivos impressos, os computadores assumindo os lugares das máquinas de escrever, os aplicativos de *smartphones* tomando os lugares de agendas físicas etc. Além disso, a forma como os lugares físicos se constitui também vem sofrendo alteração, devido aos trabalhos remotos, que permitem que escritórios em prédios corporativos se reduzam cada vez menos.

Todo esse movimento de adequação profissional aos avanços tecnológicos, essencialmente a possibilidade do trabalho à distância, acaba exigindo mais comunicações, principalmente aquelas que necessitam serem sigilosas. Nessa direção, os autores mencionam sobre as chamadas *clouds*. Essas nuvens que ficam no ciberespaço e protegidas por senhas são tentativas de proteger informações de terceiros. Como curiosidade sobre segurança de dados, os autores trazem um episódio ocorrido que envolve o vazamento de dados sigilosos.

> Um escândalo sobre segurança criptográfica abalou o mundo, quando em 2013, o analista de sistemas de computadores da CIA (*Central Intelligence Agency*, a agência de inteligência dos Estados Unidos) Edward Snowden revelou informações confidenciais, demonstrando como o governo dos EUA acessava e observava arquivos, na nuvem, da população do mundo (L_2, 2020, p. 125).

A respeito disso, ainda é sugerido ao estudante, a leitura do artigo "Entenda o caso Edward Snowden, que revelou espionagem dos EUA". Essa sugestão não é explorada nas orientações para o professor, em que os autores mencionam apenas a importância da seção "Explorando conexões" para que o professor comente com seus estudantes sobre a evolução das técnicas criptográficas diante do aumento do trabalho em *home office*.

Diante dessas discussões, compreendemos que os entrelaçamentos entre a segurança da informação e a interdisciplinaridade podem ocorrer a partir da reflexão sobre a importância do contexto histórico da criptografia, que ao transcorrer para os dias atuais são relevantes do ponto de vista da criptografia digital. Além disso, a perspectiva de observar as mudanças no mundo do trabalho, a partir da presença das tecnologias na direção dessa mudança, trazem impactos para analisar a criptografia como uma ferramenta necessária e que deve permear as funções articuladas com o trabalho exercido, como a troca de mensagens, o uso de dados de clientes ou servidores, entre outros.

6 INCOERÊNCIAS, REFLEXÕES E CONSIDERAÇÕES FINAIS

Trouxemos, neste texto, um olhar para novos LD do Ensino Médio, que estão pautados pela reforma dessa etapa escolar e pela BNCC (BRASIL, 2018). Os livros de "Ciências Humanas e Sociais Aplicadas em diálogo com a Matemática" têm um objetivo de relacionar essas áreas do conhecimento, oferecendo uma oportunidade para com o trabalho interdisciplinar. Diante disso, analisamos uma temática que, com base na literatura específica, tem relações não apenas com conceitos matemáticos, mas também com contextos históricos, incluindo aspectos políticos, militares e digitais.

Ao analisar as obras, notamos a pouca presença da criptografia na articulação entre as

áreas do conhecimento citadas. Frente às nove obras que tivemos acesso, apenas uma delas abarca discussões amplas e aprofundadas sobre o tema (L_2), enquanto outra (L_1) contempla apenas uma seção específica dentro de um capítulo com temática mais geral ("Conexões digitais"). Nessa última, parece claro o intuito de incluir a criptografia enquanto um exemplo de conexão digital possível e não com uma abordagem mais substanciada.

Contudo, mesmo que nessas obras existam discussões sobre a criptografia, algumas incoerências com conteúdos/definições foram notadas na análise. Interpretamos, por exemplo, que a definição dada sobre a criptografia digital em L_1, assim como o exemplo do cubo mágico enquanto um modo de operar com algoritmos, pode contribuir para uma confusão e compreensão inconsistente por parte do estudante. Isso ocorre, pois quando os autores definem a criptografia digital como aquela feita através de algoritmos, perde-se de vista que esses podem ser usados nas criptografias manuais ou mecânicas, ou seja, não é uma exclusividade da criptografia digital. Em nossa visão, essa decorre da utilização de computadores e da internet de modo que o processo criptográfico aconteça em frações de segundos.

Em L_2, por outro lado, no que tange às aplicações da criptografia, são exemplificados o código de barras e as cédulas de dinheiro. O primeiro é usado para permitir que empresas tenham maior controle em suas operações diárias, como monitoramento de compras e vendas; já as cédulas possuem as marcas d'água, que funcionam como a ocultação de informações presentes nas notas. Portanto, nessas situações temos as identificações de produtos por meio de uma sequência (código de barras) e ocultação de informações (marca d'água), não caracterizando a função de esconder informações, que é a premissa da criptografia.

Compreendemos que as obras poderiam apresentar em suas partes textuais, algumas relações com conceitos matemáticos, como os de função do 1º grau, que estão presentes, por exemplo, na Cifra de César, a partir do deslocamento das letras do alfabeto. Essas relações já foram evidenciadas pela literatura como sugerem alguns autores (LITOLDO, 2016; OLGIN, 2011; TAMAROZZI, 2001) . Ademais, essa abordagem poderia despertar nos estudantes um entendimento significativo deste conceito matemático ao estar atrelado com um cenário histórico e, ainda, permitir aos professores de História, Geografia e Matemática um trabalho interdisciplinar mais completo e contextualizado, além de tangenciarem outras áreas a depender do encaminhamento da discussão, por exemplo, a Sociologia e a Filosofia.

Concluímos que a presença da criptografia é pouco expressiva nos novos materiais que estão chegando às escolas. Defendemos que essa temática seja mais abordada e apresentada aos professores e estudantes, pois pode contribuir com diversos aspectos para a melhoria do ensino e da aprendizagem, como sugere a literatura. Além disso, enfatizamos que novas investigações podem ocorrer ao tomar esses livros como objetos de estudo, focando em temas, conteúdos e discussões, pois trazem iniciativas de interdisciplinaridade e precisam de reflexões da comunidade acadêmica para com o impacto desses materiais nas práticas pedagógicas dos próximos anos.

REFERÊNCIAS

AZEVEDO, E. M. d. **Livro Didático: Uma Abordagem Histórica e Reflexões a Respeito de Seu Uso em Sala de Aula**. Cadernos da FUCAMP, Monte Carmelo-MG, v. 4, n. 4, p. 1–14, 2005.

BOMFIM, F. d. S. **História da Matemática e Cinema: o caso da criptografia na introdução do ensino de Álgebra**. 2017. Dissertação (Mestrado Profissional em Ensino de Matemática) — Universidade de São Paulo, São Paulo, 2017.

BRASIL. **Lei nº 9.394, de 20 de dezembro de 1996**. Estabelece as diretrizes e bases da educação nacional. Brasília, 23 dez. 1996, 1, p. 27833.

BRASIL. **Base Nacional Comum Curricular**. Brasília: Ministério da Educação: [s.n.], 2018.

BRASIL. **Resolução n°3**, de 21 de novembro de 2018: Atualiza as Diretrizes Curriculares Nacionais para o Ensino Médio. Brasília: Ministério da Educação, 2018b.

BRASIL. **Edital de Convocação n° 03/209** - CGPLI edital de convocação para o processo de inscrição e avaliação de obras didáticas, literárias e recursos digitais para o programa nacional do livro e do material didático PNLD 2021. Brasília: Ministério da Educação, 2019a.

BRASIL. **Temas Contemporâneos Transversais na BNCC:** Contexto Histórico e Pressupostos Pedagógicos. Brasília: Ministério da Educação: [s.n.], 2019b.

BRASIL. **Guia Digital PNLD - Matemática e suas Tecnologias**. Brasília: Ministério da Educação: [s.n.], 2021a. Disponível em: <https://pnld.nees.ufal.br/pnld_2021_proj_int_vida/componente-curricular/pnld2021-didatico-matematica-e-suas-tecnologias>.

BRASIL. **Guia Digital PNLD - Obras Específicas: Ciências Humanas e Sociais aplicadas em diálogo com a Matemática**. Brasília: Ministério da Educação: [s.n.], 2021b. Disponível em: <https://pnld.nees.ufal.br/pnld_2021_didatico/inicio>.

CARVALHO, L. R. **O Uso de Elementos da Criptografia como Estímulo Matemático na Sala de Aula**. 2016. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) — Universidade Estadual Paulista, Rio Claro-SP, 2016.

CATALANO, D.; PRISCO, R. D. **Security and Cryptography for Networks**: Springer, 2018.

CHARALAMBOUS, C. Y. *et al.* A comparative analysis of the addition and subtraction of fractions in textbooks from three countries. **Mathematical thinking and learning**, Taylor & Francis, v. 12, n. 2, p. 117–151, 2010.

GOLDENBERG, M. C. d. S. M. **A arte de pesquisar: como fazer pesquisa qualitativa em Ciências Sociais**. 12. ed. Rio de Janeiro: Record, 2011.

LAJOLO, M. Livro didático: Um (quase) manual de usuário. **Em Aberto**, Brasília-DF, v. 16, n. 69, p. 2–9, 1996.

LANA, M. C. A. **Curvas elípticas e criptografia**. 2016. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) — Universidade Federal de Juiz de Fora, Juiz de Fora-MG, 2016.

LITOLDO, B. F. **As Potencialidades de uma Sequência Pedagógica de Atividades Envolvendo Problemas Criptográficos na Exploração das Ideias Associadas à Função Afim**. 2016. Dissertação (Mestrado em Educação Matemática) — Universidade Estadual Paulista, Rio Claro-SP, 2016.

LITOLDO, B. F.; LAZARI, H. Uma análise do uso da criptografia nos livros didáticos de matemática do ensino médio. **REMATEC**, v. 9, n. 17, p. 133–152, 2014.

LÜDKE, M.; ANDRÉ, M. E. D. A. **Pesquisa em Educação: Abordagens Qualitativas**. São Paulo: E.P.U., 1986.

MATIĆ, L. J. The pedagogical design capacity of lower-secondary mathematics teacher and her interaction with curriculum resources. **REDIMAT**, Hipatia Press, v. 8, n. 1, p. 53–75, 2019.

MAZZI, L. C. **As Demonstrações Matemáticas Presentificadas nos Livros Didáticos do Ensino Médio: Um Foco nos Capítulos de Geometria**. 2018. Tese (Doutorado em Ensino de Ciências e Matemática) — Universidade Estadual de Campinas, Campinas-SP, 2018.

OLGIN, C. A.; GROENWALD, C. L. O. Temas de interesse no currículo de matemática do ensino médio. In: ALME26 - ACTA LATINOAMERICANA DE MATEMÁTICA EDUCATIVA, 26., Recife, 2013. **Anais[...]**: Recife: Acta Latinoamericana de Matemática Educativa, 2013. v. 26, p. 69–78.

OLGIN, C. d. A. **Currículo no Ensino Médio: Uma Experiência com o Tema Criptografia**. 2011. Dissertação (Mestrado em Ensino de Ciências e Matemática) — Universidade Luterana do Brasil, Canoas, 2011.

PAIVA, M. *et al.* **Moderna Plus**. São Paulo: Moderna, 2020.

SANTOS, D. S. d. **Uso da Criptografia como Motivação para o Ensino Básico de Matemática**. 2015. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) — Universidade Federal de Sergipe, Itabaiana-SE, 2015.

SELKE, R. d. C. *et al.* **Dimensões**. São Paulo: FTD, 2020.

SINGH, S. **O Livro dos Códigos:** A Ciência do Sigilo - do Antigo Egito à Criptografia Quântica. 7. ed.: Rio de Janeiro: Record, 2008.

SOUZA, F. R. de. O novo ensino médio: a disputa em torno de um velho projeto formativo. **Revista Internacional Educon**, v. 2, n. 1, p. e21021004–e21021004, 2021.

SOUZA NETO, L. A. **Aritmética Modular e Criptografia no Ensino Básico**. 2014. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) — Universidade Federal do Maranhão, São Luís, 2014.

TAMAROZZI, A. C. Codificando e decifrando mensagens. **Revista do Professor de Matemática**, v. 45, p. 41–43, 2001.

VIDAL, S. C. **Criptografia como Ferramenta Educacional no Ensino da Análise Combinatória**. 2019. Dissertação (Mestrado Profissional em Projetos Educacionais em Ciências) — Universidade de São Paulo, Lorena-SP, 2019.