Anais do XVI Seminário Nacional de História da Matemática / Marcos Lübeck e Rafael Montoito (organizadores). Rio Claro/SP: SBHMat, 2025 .ISSN: 2236–4102

Pesquisas que utilizaram criptografia em diálogo com história da matemática em aliança com tecnologias digitais

Research that used cryptography in dialogue with the history of mathematics in alliance with digital Technologies

Lais Luisa Pereira da Silva[1]
Universidade Federal do Rio Grande do Norte – UFRN

Giselle Costa de Sousa[2]
Universidade Federal do Rio Grande do Norte – UFRN

RESUMO

O presente trabalho trata de um levantamento de pesquisas em periódicos com descritores específicos, tendo como objetivo apresentar estudos sobre criptografia, história da matemática (HM) e tecnologias digitais (TD), mais especificamente a criptografia de Turing e seu uso nas salas de aula em aliança com HM e TD. Portanto, adota abordagem metodológica qualitativa com procedimento bibliográfico de modo que são analisados trabalhos acadêmicos que destacam a relevância pedagógica da criptografia em diálogo com HM e TD. Para tanto, foram observados os títulos, resumos, palavras-chave, referências e corpo do texto, utilizando ainda de operadores booleanos para filtragem dos trabalhos. Além disso, esse artigo se fundamenta em estudos históricos que exploram a história da criptografia incluindo seu desenvolvimento e aplicações, como também em autores que falam a respeito da importância das tecnologias digitais para transformar práticas pedagógicas, incluindo seu potencial em aliança com história no ensino de matemática na educação básica. Como resultado, essa pesquisa conclui que, embora existam abordagens significativas para cada área individualmente, ou seja, criptografia, HM e TD, a interseção entre essas três frentes ainda é limitada, isto porque, o levantamento realizado apontou poucos trabalhos voltados para o diálogo desse terno. Contudo, a partir dos encontrados, e tendo em vista a fundamentação aqui adotada, inferimos que este trabalho contribui para a área ao delinear um panorama teórico para futuras pesquisas e aplicações práticas no campo educacional.

Palavras-chave: Criptografia; História da Matemática; Tecnologias Digitais; Ensino de Matemática; Educação Básica.

ABSTRACT

The present work deals with a survey of research in periodicals with specific descriptors, aiming to present studies on cryptography, history of mathematics (HM) and digital technologies (TD), more specifically Turing cryptography and its use in classrooms in alliance with HM and TD. Therefore, it adopts a qualitative methodological approach with a bibliographic procedure so that academic works that highlight the pedagogical relevance of cryptography in dialogue with HM and TD are analyzed. To this end, the titles, abstracts, keywords, references and body of the text were observed, also using boolean operators to filter the works. Furthermore, this article is based on historical studies that explore the history of cryptography, including its development and applications, as well as authors who talk about the importance of digital technologies for transforming pedagogical practices, including their potential in alliance with history in teaching mathematics in basic education. As a result, this research concludes that, although there are significant approaches to each area individually, that is, cryptography, HM and TD, the intersection between these three fronts is still limited, this is because the survey carried out showed few works focused on dialogue in this regard. However, based on the findings, and taking into account the reasoning adopted here, we infer that this work contributes to the area by outlining a theoretical panorama for future research and practical applications in the educational field.

Keywords: Cryptography; History of Mathematics; Digital Technologies; Teaching Mathematics; Basic Education.

[1] Mestranda no Programa de Pós-Graduação em Ensino de Ciências Naturais e Matemática da Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil. E-mail: lais.silva.700@edu.ufrn.br.

[2] Doutora em Educação pela Universidade Federal do Rio Grande do Norte (UFRN). Professora Titular da Universidade Federal do Rio Grande do Norte (UFRN), Natal, Rio Grande do Norte, Brasil. E-mail: giselle.sousa@ufrn.br.

CONSIDERAÇÕES INICIAIS

O uso da criptografia está inserido em muitos ambientes, por exemplo, tudo que possui senha ou algum tipo de segurança como bancos, cartões, redes sociais e celulares, tem criptografia para garantir o acesso aos dados somente às pessoas corretas. Dessa forma, a criptografia se faz presente no dia a dia das pessoas, em particular, dos alunos, de maneira que ensiná-la, mostrando a sua história e diferentes procedimentos/motivações de uso, pode fazer com que compreenda sua funcionalidade, incluindo em tecnologias diversas.

A criptografia se encontra de formas diferentes, em momentos variados e em múltiplas esferas distribuídas ao longo do tempo, logo, trabalhá-la por meio da história da matemática incluindo apoio de tecnologias tem potencial para ensinar ao aluno sobre como diferentes sociedades desenvolveram seus próprios métodos criptográficos utilizando ferramentas distintas, ressaltando que a criação da criptografia foi desenvolvida a partir de uma necessidade, em especial relacionada à segurança e proteção de dados. Conforme destaca Carneiro (2015, p. 3), a criptografia é definida como o estudo de "métodos ou técnicas que tornam o conteúdo de mensagens incompreensíveis às pessoas não autorizadas ao mesmo tempo permitindo que os destinatários recuperem a mensagem original". Seguiremos essa definição de criptografia, que defende que seu uso se faz por meio da busca por garantir o sigilo de informações.

Além disso, o conteúdo de criptografia com o uso de tecnologias se enquadra dentre as competências gerais da educação básica na Base Nacional Comum Curricular (BNCC), por exemplo, quando o referido documento defende que se deve:

> Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva. (Brasil, 2017, p. 8).

Com esse amparo, *o objetivo desse artigo é realizar um levantamento bibliográfico sobre criptografia, história da matemática e tecnologias digitais no ensino de matemática,* delimitando um panorama de pesquisas voltadas para essa temática que possa ser usado para fundamentação de uma pesquisa de mestrado profissional em andamento para futuro desenvolvimento de um produto educacional.

A fim de atingir este objetivo, o presente artigo é organizado em cinco seções. A primeira compreende essa introdução chamada de *Considerações iniciais*; a segunda é intitulada *Referencial* e trata dos trabalhos que embasam essa pesquisa; a terceira seção é nomeada por *Metodologia* e apresenta os meios e métodos que foram utilizados para desenvolvimento desse trabalho sendo subdividida na subseção de *Seleção de repositórios* e subseção de *Seleção de descritores, filtragem, observação e seleção de arquivos*; a quarta sessão é intitulada de *Análise e Resultados* de modo que, nela, discutimos acerca da pesquisa e implicações que nos levou, estando subdividida na subseção de título *Uma história da criptografia* e a subseção com título *Alan Turing* as quais se destinam, a partir dos achados, a descrever uma breve narrativa histórica sobre o assunto; por fim, a quinta seção que traz as *Conclusões*, na qual fazemos um aparato geral sobre objetivos alcançados e desdobramentos futuros.

Desse modo, trazemos na próxima seção uma discussão sobre o referencial da pesquisa aqui desenvolvida.

REFERENCIAL

Considerando que esta pesquisa tem como objeto um diálogo entre a criptografia, sua história e as tecnologias digitais em prol do ensino de matemática, seus fundamentos residem em categorias de referenciais que tratam de cada um desses pontos. De fato, buscamos referencial em documentos que regem a educação básica, a exemplo da Base Nacional Comum Curricular – BNCC – complementar (2022) e BNCC (2017). Além disso, procuramos nos fundamentar em referenciais que tratam da história da matemática, em especial da criptografia como Khan (1967). Também encontramos bases em referencias sobre tecnologias digitais e seu uso no ensino, a exemplo de Borba (2010). Assim como na aliança entre história da matemática (HM) e tecnologias digitais (TD), defendida por Sousa (2020, 2023, 2024).

Esclarecendo, o presente trabalho aborda a importância do uso de tecnologias digitais, em prol do ensino, em diálogo com história da matemática ligada à criptografia, uma área que combina conceitos matemáticos com aplicações práticas. Para estudo deste tema, se faz necessária uma fundamentação sobre o uso de recursos tecnológicos e da história da matemática na educação, como meio de compreensão para o uso da criptografia e como mediação no ensino da matemática, além dos fundamentos da criptografia no contexto pedagógico, em especial, da educação básica.

Como dito, podemos encontrar tal respaldo na BNCC (Brasil, 2017) que incentiva o uso, a compreensão e a criação de tecnologias. Além disso, temos um documento complementar a BNCC, intitulado *Computação na Educação Básica* (Brasil, 2022), que além de defender o uso das tecnologias, traz consigo justificativas também para o ensino da criptografia na educação básica. Na habilidade (EF09CO05) nomeada *Analisar técnicas de criptografia para armazenamento e transmissão de dados*, há exemplos de como trabalhar a criptografia neste nível de ensino, por exemplo:

> (1) Apresentando o conceito de criptografia, por exemplo, usando algoritmos simples de criptografia para que os estudantes codifiquem textos e frases e troquem mensagens criptografadas com os colegas. (2) Discutindo a importância do tráfego de informações criptografadas nas redes, por exemplo, em relação a dados como senhas e informações bancárias das pessoas. (3) Discutindo o papel histórico da criptografia, por exemplo, na comunicação de informações sigilosas durante a Segunda Guerra Mundial. (Brasil, 2022, p. 55).

Ainda nesse documento temos outros exemplos de uso da criptografia e argumentos que respaldam a abordagem dessa temática na educação básica, em especial no ensino de matemática.

Os fundamentos supracitados se apoiam numa definição de criptografia que se assemelha a de Khan (1967) que diz que os métodos de criptografia, não ocultam a presença de uma mensagem secreta, mas a tornam ininteligível para estranhos por meio de diversas transformações do texto simples. Tal definição se ancora em uma narrativa historiográfica da criptografia, a fim de compreendê-la. Assim, Khan (1967) também descreve uma história da criptografia contando sobre as primeiras aparições dos mecanismos, acerca de três mil anos antes de Cristo, e passando pelas demais até sua época. Encontramos nesta história fundamentos para o nosso trabalho em reconhecer a importância da história, em particular, da criptografia, a fim de usá-la como ferramenta de ensino, como almejamos.

Diante da história da criptografia e elucidação de sua definição, a relação íntima com tecnologias é revelada de forma que procuramos também em nosso trabalho referenciais que testifiquem seu uso em sala de aula. Nesta direção, Borba (2010) coloca que as possibilidades proporcionadas pelos *softwares* têm o potencial de modificar tanto o tipo de atividades propostas em sala de aula quanto a própria natureza do conhecimento matemático, permitindo uma transformação significativa no ensino e na aprendizagem da disciplina. Essa perspectiva destaca o impacto das tecnologias digitais no ambiente educacional e no papel do professor em adaptar-se a essas novas ferramentas.

Além de aspectos da história da matemática e das tecnologias como ferramentas de ensino, pretendemos também usar ambas trabalhando em consonância, uma aliança defendida em trabalhos de Sousa (2020, 2023, 2024), os quais exploram as chances de usar a história da matemática (HM) e tecnologias digitais (TD) ao ensino de matemática de modo aliado, apresentando fundamentos e atividades, como sequências didáticas. Para tanto, por exemplo, cita argumentos de Fauvel e Maanen (2002, *apud* Sousa, 2020, p. 26) como:

> [...] calculadoras programáveis modernas permitem que os estudantes de hoje refaçam os cálculos de antigamente, muitas vezes, para maior precisão e muito mais para o cálculo. Capturado em poucos segundos um cálculo pode ter levado dezesseis séculos, dias ou meses dos astrônomos, os alunos não vão indiscutivelmente recapturar a experiência antiga, mas gerar uma nova. Em alguns casos, os estudantes de hoje podem ser capazes de encontrar coisas nas imagens que os antecessores não puderam.

A aliança entre HM e TD possui um potencial de ensino baseado na história da matemática, essa aliança que dantes era uma tríade junto com a investigação matemática pode ser trabalhada em dupla entre a HM e a TD como explica Sousa (2023, p. 113):

> A aliança consiste em uma tendência de educação matemática que conectou, inicialmente HM e TD via IM em prol do ensino, mas que a tríade se desdobra no par de aliança entre HM e TD que podem ser via outras tendências para além da IM, bem como, permite mais conexões.

Dessa maneira, pretendemos abordar um diálogo entre a criptografia, a HM e as TD no ensino da matemática, discutindo o uso dessas ferramentas no ensino da matemática. Para tanto, buscamos trabalhos a respeito, destinando tal processo na próxima seção onde serão detalhados os procedimentos metodológicos usados para realizar este levantamento.

METODOLOGIA

A abordagem metodológica adotada neste artigo é qualitativa, pois se baseia na percepção humana, definição trazida por Stake (2011). Logo, esse estudo procura além de ver a quantidade de trabalhos na área, identificar pontos significativos para nossa pesquisa tendo em vista nosso objetivo e fundamentos.

Dentro da abordagem qualitativa adotamos, neste artigo, o procedimento bibliográfico no qual, de acordo com Stake (2011), há uma busca de documentos associada a uma interpretação desses, analisando e sintetizando os dados coletados e aumentando nossa experiência e percepção sobre nosso objeto de investigação. Em seus procedimentos temos a coleta e a interpretação dos epi-

sódios, por exemplo, trechos, citações, traduções de bibliografias, bem como, imagens e associação destes elementos.

Esclarecendo, neste artigo, o levantamento foi realizado em cinco etapas para seleção e observação de quantidade e semelhança de trabalhos tendo em vista os anseios da pesquisa. As cinco etapas foram:

1) Seleção dos repositórios;
2) Seleção dos descritores (que foram buscados em alguns casos em inglês);
3) Filtragem e combinação de descritores;
4) Observação de arquivos relacionados;
5) Seleção de documentos/bibliografias que se direcionam ao nosso objeto de pesquisa (diálogo entre criptografia, história da matemática e tecnologias digitais no ensino de matemática).

Seleção dos Repositórios

Foram selecionados quatro repositórios digitais, cada um escolhido por uma característica particular, mas de modo a abarcar bibliografias acadêmicas do tipo livros, tese, dissertação e artigo científico, que foram os tipos encontrados no decorrer da pesquisa. São eles:

O CREPHIMAT[3] – Centro Brasileiro de Referência em Pesquisa sobre História da Matemática – é voltado a pesquisas na área da história da matemática. Dessa forma, ao pesquisar nele já sabemos que os trabalhos que serão encontrados possuem uma abordagem histórica, que coincide com anseio de nossa pesquisa.

Periódicos da Capes[4] – Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – é repositório onde trabalhos acadêmicos, incluindo produções de mestrado e doutorado, podem ser obtidos, contendo os estudos realizados no Programa de Pós-graduação em Ensino de Ciências Naturais e Matemática (PPGECNM) ao qual estamos vinculados. Assim, é uma biblioteca de buscas primárias para observar modelos, linhas de pesquisas e produtos da área pesquisada.

Google Acadêmico[5] foi escolhido por ser uma biblioteca digital mais ampla de trabalhos científicos, de modo que a busca nela exige mais filtros, já que possui um acervo maior de artigos, teses, dissertação, resumos e livros.

Por fim o *banco de dados Scielo*[6] – *Scientific Eletronic Library Online*–foi escolhido por ser um banco com visibilidade internacional. Neste caso, algumas das buscas foram, inclusive, feitas em inglês.

[3] Acesso através do link: https://www.crephimat.com.br/ . Último acesso em 17, nov. 2024.
[4] Acesso através do link: https://www.periodicos.capes.gov.br/ . Último acesso em 17, nov. 2024.
[5] Acesso através do link: https://scholar.google.com.br/?hl=pt . Último acesso em 17, nov. 2024.
[6] Acesso através do link: https://www.scielo.br/ . Último acesso em 17, nov. 2024.

Seleção dos descritores, filtragem, observação e seleção de arquivos

Os descritores selecionados foram: criptografia (*encryption*), história da matemática (*history of math*), tecnologia (*technology)*, matemática (*math*) e Alan Turing[7], que estão relacionados diretamente a temática desta pesquisa. A seleção e a filtragem dos descritores foram realizadas a partir de combinações do descritor *criptografia* com os demais, fazendo uso dos operadores booleanos[8] (*AND, OR e NOT*) com base na relevância para os objetivos da pesquisa e no número de resultados obtidos. As buscas foram realizadas no período de outubro a novembro de 2024. A partir da observação preliminar da quantidade de documentos retornados, a leitura foi direcionada, mediante os descritores apresentados e a finalidade exibida nos resumos, exclusivamente para aqueles que se alinhavam mais estreitamente à temática investigada (ligação entre criptografia, história da matemática, tecnologias digitais e ensino de matemática). Este alinhamento foi avaliado pela presença e pertinência dos descritores nos trabalhos encontrados por meio do comando *AND* que seleciona os documentos que falam da combinação dos descritores.

Arquivos/bibliografias que apresentavam maior número de descritores relevantes foram priorizados, como o escrito por Vizioli, Carvalho e Pereira (2019) que falam da possibilidade do uso da criptografia para o ensino de função inversa utilizando a tecnologia como ferramenta para tal. Assim, temos um exemplo de trabalho com uso da criptografia e a tecnologia voltado para o ensino, porém a busca foi mais voltada especialmente **à**queles relacionados à história da matemática, que se mostrou um dos descritores menos frequentes. Para tanto, foram selecionados os descritores *criptografia and história da matemática*. Como resultado, com exceção do *Google Acadêmico*, foi possível encontrar no máximo um documento por periódico/repositório, nas buscas realizadas.

Adotando os procedimentos supracitados, no *CREPHIMAT* somente uma dissertação foi encontrada utilizando apenas o descritor *criptografia.* Nesse trabalho temos a criptografia sendo utilizada por meio do cinema. O trabalho encontrado é de autoria de Fabiana de Souza Bonfim e tem como título *História da matemática e cinema: o caso da criptografia na introdução do ensino de álgebra*, sendo defendido no ano de 2012. Segundo Bonfim (2012), o uso da história da matemática associado ao cinema pode ser uma ferramenta eficaz na introdução de conceitos de álgebra, como demonstrado no caso da criptografia. Essa abordagem permite contextualizar os conteúdos matemáticos e torná-los mais significativos para os alunos, explorando conexões históricas e aplicações práticas do tema no ensino (Bonfim, 2012).

Nos *Periódicos da Capes* a busca por *criptografia* trouxe 247 resultados, sendo assim se fez necessária uma filtragem com acréscimo dos outros descritores. Adicionando *história da matemática*, apenas um arquivo foi encontrado. O trabalho obtido é *Criptologia: possibilidade de estudo no ensino médio amparada em sua concepção histórica* de autoria de Gomes, Santos e Lopes (2016). Neste caso, os referidos autores argumentam que a criptologia pode ser incorporada ao ensino médio como uma ferramenta pedagógica para conectar a história da matemática com conceitos contemporâneos. Essa abordagem permite contextualizar o conteúdo de forma interdisciplinar, promovendo o engajamento dos alunos ao explorar tanto aspectos históricos quanto aplicações práticas da matemática.

Com os descritores *criptografia*, *tecnologia* e *matemática*, seis arquivos foram obtidos nos *Periódicos da Capes* sendo observado que são direcionados para o ensino de criptografia na etapa do

[7] Alan Turing (1912-1954) foi um inglês que se dedicou à matemática e à criptografia, sendo considerado um dos precursores da computação, entre outras contribuições. Mais detalhes serão tratados adiante neste texto.

[8] Palavras que indicam ao sistema de busca como combinar os termos de uma pesquisa.

ensino médio. São eles: *Tecnologias digitais aliadas ao ensino de Criptografia,* de Silva, Evangelista e Evangelista (2022); *Criptologia: possibilidade de estudo no ensino médio amparada em sua concepção histórica,* de Gomes, Santos e Lopes (2016); *Construção de conhecimentos matemáticos utilizando a temática criptografia para o Ensino Médio,* de Kranz e Olgin (2021); *Criptografia simétrica com uma função afim,* de Menezes Neto e Mota (2023); *Criptografia e Livros Didáticos do Ensino Médio: Uma Análise Sobre as Novas Obras Didáticas Específicas do PNLD 2021,* de Litoldo e Guimarães (2023); e *Engenharia didática: uma experiência com o tema criptografia,* de Olgin e Groenwald (2011).

Ainda nos *Periódicos da Capes*, a busca utilizando *criptografia* e *Alan Turing* não obteve nenhum resultado, porém, quando pesquisado em inglês, apareceram 15 trabalhos, filtrando com *Alan Turing*, *history of mathematics* e *encryption* aparece um arquivo. Tal trabalho é de autoria de William H. Sherman e intitulado *Decoding Early Modern Cryptography.* Nele, Sherman (2019) explora como a criptografia, durante a era moderna, foi não apenas uma ferramenta prática para proteger mensagens, mas também um reflexo cultural e intelectual do período. Ele analisa os métodos criptográficos usados na época e os contextualiza em práticas sociais e políticas, destacando como esses sistemas influenciaram e foram influenciados pelas ideias emergentes de linguagem, ciência e segurança. Nesse trabalho foi possível encontrar outras referências importantes da área da criptografia como o livro *The Codebreak* (Kahn, 1967) que traz uma história ampla da criptologia e fundamenta este artigo a dissertação a qual tal estudo é vinculado.

A pesquisa realizada no *Google Acadêmico* foi mais volumosa, de fato, foram encontrados para o descritor *criptografia*, 26100 documentos, isso sem as citações. Mesmo com todos os descritores usados juntos, através dos operadores, ou seja, *criptografia*, *Alan Turing*, *tecnologias* e *história da matemática*, foram obtidos 35 resultados. Da seleção alcançada, para este artigo, foram revisadas as referências dessas 35 bibliografias a fim de fomentar nossa fundamentação sobre o assunto. Contudo, como desdobramento deste artigo, para a dissertação a ele vinculada, serão analisados o conteúdo dos estudos que têm um enfoque no uso da história da matemática e das tecnologias como ferramentas para o ensino.

Por fim, na *base de dados da Scielo* apareceram dez resultados para *criptografia,* porém, para o conjunto com *história da matemática* não foi encontrado nenhum resultado. Assim, foi feita uma busca com os mesmos descritivos em inglês e o resultado foi o mesmo, isto é, nenhum arquivo na base de dados da Scielo se assemelha a pesquisa dissertativa em andamento e ao objeto deste artigo.

Consideramos que o levantamento realizado permite delinear amparo teórico e delimitar o campo de relação entre criptografia, história da matemática e tecnologias digitais em prol do ensino. Uma análise mais detalhada e apontamentos dos achados pode ainda desenhar uma história da criptografia com a intenção de usá-la em aliança com tecnologias para o ensino, como descrevemos na seção que segue.

ANÁLISES E RESULTADOS

Nesta seção, serão apresentados os resultados obtidos com base nas pesquisas realizadas, seguidos de sua análise à luz do referencial adotado. Mediante o que foi observado, os trabalhos selecionados falam de criptografia, seja por meio da história da matemática, seja por meio de tecnologias digitais, trazendo abordagens voltadas para o ensino da matemática no ensino médio.

Com base nos resultados das buscas realizadas, observa-se que muitos trabalhos se concentram no estudo da criptografia, no entanto, o número de pesquisas que abordam a matemática associada a história da matemática e tecnologias é significativamente menor. Nesse contexto, a presente pesquisa representa uma contribuição relevante, considerando a escassez de trabalhos que integram essas abordagens, podendo servir como referência para outros profissionais da área que desejem implementar propostas nesta direção. Dentre as contribuições dos trabalhos selecionados e, tendo em vista, os anseios deste artigo e natureza do evento ao qual está direcionado, XVI Seminário Nacional de História da Matemática, destacamos a identificação de uma bibliografia clássica sobre criptografia e sua história, o livro de David Kahn, *The Codebreakers*, publicado em inglês em 1967. Disponível em formato digital, a obra está dividida em 26 capítulos e apresenta, entre os capítulos 2 e 19, uma narrativa detalhada sobre a história da criptologia – ciência que abrange a criptografia e a criptoanálise (que em geral consiste no processo de tentar descobrir o texto cifrado). Detalhando seu conteúdo e adotando como principal referencial, decidimos esboçar uma história da criptografia e contribuições de Alan Turing nas próximas duas subseções.

Uma história da criptografia

A obra de David Khan (1967), com o título *The Codebreakers: the story of secret writing,* relata as principais fases da história da criptografia de forma detalhada. Desse modo, revela o desenvolvimento dessa ferramenta em momentos diversos e culturas distintas, desde as primeiras evidências de criptografia, acerca de 4000 anos atrás, até a criptografia eletrônica, criada e utilizada por militares na época da guerra fria, no entanto, a obra não as criptografias atuais[9], devido à época de sua divulgação. De fato, Khan (1967, p. 9, tradução própria) descreve como objetivo do seu livro "abranger toda a história da criptologia. Meu objetivo foi duplo: narrar o desenvolvimento dos diversos métodos de criação e quebra de códigos e cifras, e contar como esses métodos afetaram as pessoas."[10], sendo uma obra ampla para quem busca entender os fundamentos da criptografia.

Segundo o autor, as primeiras obras sobre o assunto aparecem no antigo Egito, através de papiros encontrados nas catacumbas, que utilizavam símbolos para ocultar informações (anexo I), passando também pelas criptografias gregas e romanas, a exemplo da criptografia de César (anexo II), que desloca as posições das letras no alfabeto para criar mensagens criptografadas e do quadro de Políbio (anexo III), que utilizada números para cifrar uma mensagem. Na era medieval, a criptografia começou a ser utilizada pela igreja e por reinos para proteger mensagens importantes. Após, métodos mais sofisticados, como cifras polialfabéticas, começaram a emergir, preparando o terreno para avanços técnicos, a exemplo temos o disco cifrado de Leon Battista Alberti (anexo IV).

No decorrer dos anos, segundo Khan (1967), épocas como o Renascimento (século XIV a XVII) e Revolução Científica (entre os séculos XVI e XVIII), também apresentam desenvolvimento acerca das criptografias, com a introdução de métodos mais complexos, como a cifra de Vigenère (anexo V). Aqui, a criptografia começa a se expandir com a influência de matemáticos e o surgimento de ferramentas mais avançadas para análise e construção de códigos. Com o advento da Revolução Industrial (entre séculos XIX e XX), novas tecnologias, como o telégrafo[11], demandaram avanços significativos na criptografia. Durante a Primeira e Segunda Guerras Mundiais, a cripto-

[9] Criptografia de chave pública, como o RSA, e padrões como o AES, que são fundamentais para a segurança digital moderna.

[10] *"The book seeks to cover the entire history of cryptology. My goal has been twofold: to narrate the development of the various methods of making and breaking codes and ciphers, and to tell how these methods have affected men."*

[11] Telégrafo é um aparelho que era utilizado para a comunicação em partes do século XIX e do século XX. Esse equipamento utilizava a energia elétrica para enviar pulsos na corrente que eram interpretados por meio de um código que usava pontos e linhas.

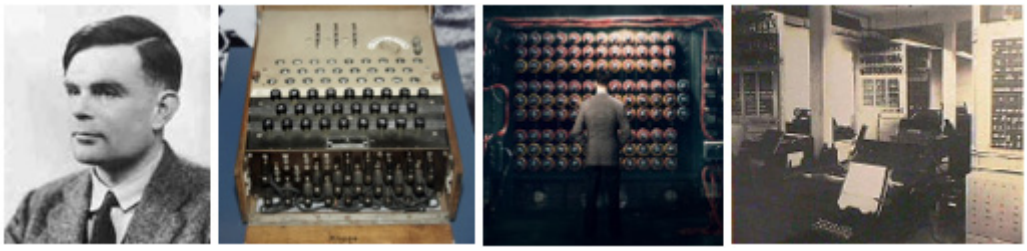
grafia alcançou novos patamares, sendo usada amplamente em operações militares. Destaca-se a batalha entre os códigos dos Aliados e do Eixo[12], incluindo o impacto do trabalho de Alan Turing e a decodificação da máquina Enigma[13]. No texto de Khan (1967), há muitos relatos sobre a guerra, porém, não há muitas menções a Alan Turing, para saber mais sobre ele, foi necessária a busca na Biblioteca Digital Britânica, em conjunto com outras fontes, como o site Mactutor[14], cujos dados detalhamos posteriormente.

Por fim, no livro, Khan (1967) descreve a criptografia que foi utilizada durante e após a Guerra Fria, tornando-se central para a segurança nacional e culminando com o desenvolvimento de sistemas como o *National Security Agency* (NSA). É ressaltado que as técnicas se tornaram mais dependentes de máquinas e algoritmos, avançando para o uso em larga escala, com aplicações em comunicações diplomáticas e espionagem. Dessa forma, utilizamos a obra para realizar um estudo das principais criptografias de cada época, pois David Kahn (1967) documenta não apenas os métodos, mas também as figuras históricas e os contextos sociais e políticos que moldaram o desenvolvimento da criptografia. Seu trabalho é considerado uma referência fundamental para o estudo da história dessa área, porém, conforme mencionado, não explora muito a figura de Alan Turing, do qual iremos falar a seguir.

Alan Turing

De acordo com Copeland (2024), Alan Mathison Turing nasceu em 23 de junho de 1912, em Londres, Inglaterra. Reconhecido como um matemático de destaque do século XX, Turing realizou contribuições significativas para diversas áreas, como criptoanálise, lógica, filosofia, biologia, matemática e ciência da computação. Ele é amplamente reconhecido como pioneiro da inteligência artificial e criador de conceitos que moldaram a computação moderna. Sua contribuição mais conhecida foi o desenvolvimento da máquina capaz de decifrar os códigos gerados pela complexa máquina alemã Enigma, como consta na Figura 1, um marco histórico na Segunda Guerra Mundial.

Figura 1 – Alan Turing e máquinas Enigma, Bombe e Tunny



Fonte: Connor e Robertson (2003); Fernandes (2024); Amorin (2020); Novo Milênio (1997)

Turing estudou em escolas de excelência e, em 1931, ingressou na Universidade de Cambridge para estudar matemática, onde se destacou por suas pesquisas em teoria da probabilidade e outros temas fundamentais para o avanço da computação. Posteriormente, mudou-se para Princeton, onde concluiu seu doutorado em lógica matemática, consolidando-se como um dos principais intelectuais da época. Durante a Segunda Guerra Mundial,

[12] Aliados e Eixo foram as duas principais alianças durante a Segunda Guerra Mundial (1939-1945).
[13] Enigma foi uma máquina de criptografia eletromecânica usada pelos alemães na Segunda Guerra Mundial para enviar mensagens codificadas.
[14] https://mathshistory.st-andrews.ac.uk/

Turing liderou esforços para decifrar os códigos alemães, projetando a máquina Bombe[15] (Figura 1), que foi crucial para a interceptação e interpretação de mensagens codificadas pelos alemães. Esse trabalho deu uma vantagem estratégica decisiva aos aliados. Ele também desenvolveu métodos inovadores para decifrar a máquina Tunny[16] (Figura 1), outro sistema alemão de cifras. Por sua contribuição, Turing foi condecorado como Oficial da Ordem do Império Britânico (OBE).

Apesar de seu impacto histórico, Turing enfrentou preconceito e perseguição por sua orientação sexual. Ele foi submetido a um tratamento hormonal, conhecido como castração química, o que o levou a um profundo sofrimento psicológico. Em 1954, Turing faleceu, possivelmente por suicídio, após ingerir cianeto. Trabalhar a figura de Alan Turing na educação básica é essencial não apenas por sua relevância científica e histórica, mas também pelo exemplo que oferece sobre a importância da inclusão e do respeito à diversidade. Sua trajetória inspira o pensamento crítico, a inovação tecnológica e a valorização dos direitos humanos, tornando-se um tema interdisciplinar ideal para conectar matemática, história, tecnologia e ética. Considerando a breve história descrita, a partir dos achados do levantamento realizado, trazemos, na sequência, nossas conclusões conforme consta próxima seção.

CONSIDERAÇÕES FINAIS

Os resultados obtidos evidenciam a relevância da abordagem interdisciplinar entre criptografia, história da matemática e tecnologias digitais no ensino de matemática. Identificou-se uma lacuna significativa na literatura acadêmica que une essas três frentes de forma integrada, reforçando a importância deste levantamento para ampliar o escopo de pesquisas futuras. Ao trabalhar a criptografia com suporte histórico e tecnológico, pode-se proporcionar ao aluno não apenas o aprendizado matemático, mas também uma compreensão crítica e contextualizada do uso das tecnologias e seu papel na história da sociedade. Isso se alinha às competências gerais da Base Nacional Comum Curricular (Brasil, 2017; 2022), que destacam a necessidade de compreender, criar e utilizar tecnologias digitais de forma ética e significativa.

Além disso, a pesquisa destacou a importância de referências históricas, como a obra *The Codebreakers,* de David Kahn (1967), bem como de figuras como Alan Turing, cuja trajetória oferece lições de inovação e inclusão. Essa perspectiva interdisciplinar é fundamental para desenvolver estratégias pedagógicas inovadoras que engajem os estudantes e conectem o conteúdo curricular à realidade contemporânea. Em suma, este trabalho não apenas contribui para reflexões teóricas sobre a integração entre criptografia, história da matemática e tecnologias digitais, mas também serve como base para o desenvolvimento de práticas educacionais que possam ser amplamente aplicadas na educação básica, a exemplo da dissertação e produto educacional vinculados e como desdobramento deste artigo.

REFERÊNCIAS

AMORIN, Gabriel. (2020). 1 jan 1939 ano–Alan Turing faz o desenho inicial da Bombe. In: **The time.graphics**. Disponível em: https://time.graphics/pt/event/4631682. Acesso em: 28 dez. 2024.

[15] Bombe, máquina eletromecânica de quebra de códigos criada por criptologistas na Grã-Bretanha durante a Segunda Guerra Mundial

[16] Tunny foi um dispositivo usado para quebrar mensagens criptografadas pelos alemães e fornecer informações importantes para as forças aliadas

BRASIL. Ministério da Educação. **Computação na Educação Básica – Complemento à BNCC**. Brasília, DF: MEC, 2022. Disponível em: https://portal.mec.gov.br/docman/fevereiro-2022-pdf/236791-anexo-ao-parecer-cneceb-n-2-2022-bncc-computacao/file. Acesso em: 7 nov. 2024.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, DF: MEC, 2017. Disponível em: http://basenacionalcomum.mec.gov.br/. Acesso em: 7 nov. 2024.

BONFIM, Fabiana de Souza. **História da Matemática e Cinema: o caso da criptografia na introdução do ensino de álgebra.** Orientador: Antônio Carlos Brolezzi. São Paulo: USP, 2012.

BORBA, Marcelo de Carvalho. Softwares e internet na sala de aula de matemática. In: **Encontro Nacional de Educação Matemática**, 10., 2010, Salvador-BA. Disponível em: <www.rc.unesp.br/gpimem/downloads/artigos/borba/marceloxenen.PDF> . Acesso em: 22 dez. 2024.

CARNEIRO, Framilson José Ferreira. **Criptografia e a Teoria dos Números**. São Paulo: Editora Ciência Moderna, 2015.

CONNOR, John O'.; ROBERTSON, Edmund. (2003). **Alan Mathison Turing.** In: Mactutor.

Disponível em: https://mathshistory.st-andrews.ac.uk/Biographies/Turing/. Acesso em 28 dez. 2024.

COPELAND, Jack B. (2024). In: **Encliclopaedia Britannica**. Alan Turing. Disponível em: https://www.britannica.com/biography/Alan-Turing. Acesso em: 21 dez. 2024.

GOMES, Francisco Claudio Lima; SANTOS, Leniedson Guedes dos; LOPES, Thiago Beirigo. CRIPTOLOGIA: POSSIBILIDADE DE ESTUDO NO ENSINO MÉDIO AMPARADA EM SUA CONCEPÇÃO HISTÓRICA. **Boletim Cearense de Educação e História da Matemática**, [S. l.], v. 3, n. 9, p. 63–78, 2016. DOI: 10.30938/bocehm.v3i9.54. Disponível em: https://revistas.uece.br/index.php/BOCEHM/article/view/54. Acesso em: 1 nov. 2024.

FERNANDES, Cláudio. Máquina Enigma. (2024). In: **Brasil Escola.** Disponível em: https://brasilescola.uol.com.br/historiag/maquina-enigma.htm. Acesso em 28 de dezembro de 2024.

KAHN, David. **The Codebreakers:** The Story of Secret Writing. Nova York: Macmillan, 1967. ISBN: 9780684831305.

KRANZ, Bárbara Elisa; OLGIN, Clarissa de Assis. Construção de conhecimentos matemáticos utilizando a temática criptografia para o Ensino Médio. **Revista de Ensino de Ciências e Matemática**, São Paulo, v. 12, n. 3, p. 1–21, 2021. DOI: 10.26843/rencima.v12n3a24. Disponível em: https://revistapos.cruzeirodosul.edu.br/rencima/article/view/2877. Acesso em: 1 nov. 2024.

LITOLDO, Beatriz Fernanda; GUIMARÃES, Douglas Ribeiro (2023). Criptografia e Livros Didáticos do Ensino Médio. **Abakós**, *11*(2), 31-51. https://doi.org/10.5752/P.2316-9451.2023v-11n2p31-51

MENEZES NETO, Jose Laudelino de; MOTA, Welisson Martins. Criptografia simétrica com uma função afim. C.Q.D.–**Revista Eletrônica Paulista de Matemática**, Bauru, v. 23, n. 1, p. 99–110, 2023. DOI: 10.21167/cqdv23n12023099110. Disponível em: https://sistemas.fc.unesp.br/ojs/index.php/revistacqd/article/view/362. Acesso em: 25 nov. 2024.

NOVO Milênio. In: **Caderno Informática** do jornal A Tribuna. Santos/SP, em 9 de setembro de 1997. Disponível em: https://www.novomilenio.inf.br/ano97/97hist03.htm. Acesso em: 28 dez. 2024.

OLGIN, Clarissa de Assis; GROENWALD, Claudia Lisete de Oliveira. Engenharia didática: uma experiência com o tema criptografia. **JIEEM – Jornal Internacional de Estudos em Educação Matemática**, 2011.

SHERMAN, William Henry. "Decoding Early Modern Cryptography." **Huntington Library Quarterly**, vol. 82 no. 2, 2019, p. 315-319. Project MUSE, https://dx.doi.org/10.1353/hlq.2019.0017.

SILVA, M. V. da .; EVANGELISTA, D. H. R.; EVANGELISTA, C. J. . Digital technologies combined with teaching Cryptography. **The Journal of Engineering and Exact Sciences**, Viçosa/MG, BR, v. 8, n. 5, p. 14313–01e, 2022. DOI: 10.18540/jcecvl8iss5pp14313-01e. Disponível em: https://periodicos.ufv.br/jcec/article/view/14313. Acesso em: 13 feb. 2025.

SOUSA, Giselle Costa de. **Aliança entre História da Matemática e Tecnologias via Investigação Matemática.** 1ª ed. São Paulo: Editora Livraria da Física, 2020. 270 p. ISBN 9786555630114.

SOUSA, Giselle Costa de. **Aliança entre história da matemática e tecnologias digitais na educação matemática.** São Paulo: Livraria da Física, 2023.

SOUSA, Giselle Costa de. Aliança entre História da Matemática e Tecnologias Digitais na Perspectiva da Teoria da Objetivação: um levantamento bibliográfico. **PARADIGMA**, Maracay, v. 45, n. 2, p. e2024010, 2024. DOI: 10.37618/PARADIGMA.1011-2251.2024.e2024010.id1583. Disponível em: https://revistaparadigma.com.br/index.php/paradigma/article/view/1583. Acesso em: 13 feb. 2025.

STAKE, Robert Earl. Pesquisa Qualitativa. Cap. 1 – **Pesquisa qualitativa como as coisas funcionam.** Cap. 2 – Interpretação a pessoa como instrumento. Porto Alegre: EDITORA PENSO, 2011.

VIZOLLI, Idemar; CARVALHO, Euvaldo de Souza.; PEREIRA, Onésimo Rodrigues. CRIPTOGRAFIA: UMA POSSIBILIDADE PARA O ENSINO DE FUNÇÃO INVERSA. REAMEC– **Rede Amazônica de Educação em Ciências e Matemática**, Cuiabá, Brasil, v. 7, n. 1, p. 196–212, 2019. DOI: 10.26571/REAMEC.a2019.v7.n1.p196-212.i8146. Disponível em: https://periodicoscientificos.ufmt.br/ojs/index.php/reamec/article/view/8146. Acesso em: 1 nov. 2024.

ANEXOS

Anexo I – Símbolos para ocultar informações

Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right

Fonte: Khan (1967, p. 73).

Anexo II – Criptografia de César

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

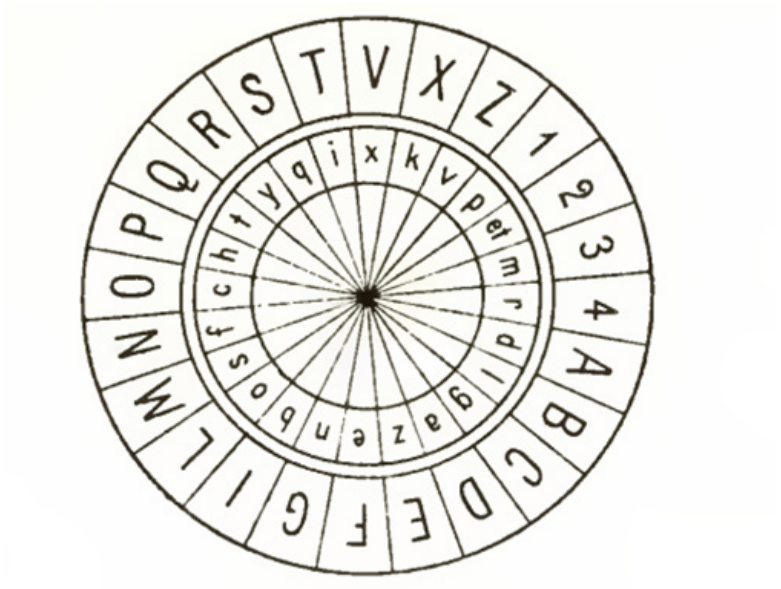
Fonte: Khan (1967, p. 84).

Anexo III – Quadro de Políbio

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Fonte: Khan (1967, p. 83).

Anexo IV – Disco cifrado de Leon Battista Alberti



Fonte: Khan (1967, p. 128).

Anexo V – Cifra de Vigenère

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	C	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Khan (1967, p. 149).