RENCIMA
Revista de Ensino de Ciências e Matemática

eISSN 2179-426X
10.26843/rencima.v12n3a24

Construção de conhecimentos matemáticos utilizando a temática criptografia para o Ensino Médio

Bárbara Elisa Kranz[1]

Clarissa de Assis Olgin[2]

***Resumo*:** Com a utilização intensa das tecnologias digitais pela sociedade, a privacidade e seguridade das informações transmitidas entre os indivíduos via internet se faz cada vez mais necessária. É nesse cenário que a criptografia torna-se essencial, pois possibilita que dados sejam compartilhados de forma segura por esses meios. Dessa forma, entende-se que esse tema tem potencial para ser explorado em sala de aula, em especial no ensino de Matemática. O objetivo deste artigo é apresentar as contribuições de uma sequência didática com a utilização de planilhas eletrônicas do Excel envolvendo o tema criptografia e o conteúdo de matrizes do Ensino Médio. Trata-se de uma de investigação matemática, desenvolvida com seis estudantes do 3° ano do Ensino Médio, de uma escola pública, no estado do Rio Grande do Sul (Brasil). Os dados foram obtidos por meio da aplicação de questionários, registros escritos e arquivos salvos em planilhas eletrônicas, os quais oportunizaram analisar a proposta didática. Com base nesses registros, constata-se que é possível trabalhar o conteúdo de matrizes de forma contextualizada e aliada a utilização de planilhas eletrônicas. Por meio deste estudo, conclui-se que a elaboração de atividades contextualizadas pode contribuir para o desenvolvimento do conteúdo de matrizes e, ainda, a utilização das planilhas eletrônicas, como recurso tecnológico, pode ser um facilitador para o processo de ensino e aprendizagem dos estudantes do Ensino Médio.

Palavras-chave: Currículo de Matemática. Ensino Médio. Matrizes. Criptografia. Planilhas Eletrônicas.

Construction of mathematical knowledge using the cryptography theme for High School

Abstract: With the intense use of digital technologies by society, the privacy and security of information transmitted between individuals by the internet is becoming increasingly necessary. In this scenario that encryption becomes essential, as it allows data to be securely shared by these means. Thus, it is understood that this topic has the potential to be explored in the classroom, especially in the teaching of mathematics. The purpose of this article is to present the contributions of a didactic sequence using Excel spreadsheets involving the theme cryptography and the matrices, a high school content. It is a mathematical investigation, developed with six students from the 3rd year of high school, from a public school, in the state of Rio Grande do Sul (Brazil). The data were obtained through the application of questionnaires, written records and files saved in electronic spreadsheets, which made it possible to analyze the didactic proposal. Based on these records, it appears that it is possible to work on the content of matrices in a contextualized way and combined with the use of electronic spreadsheets. Through this study, it is

[1] Licenciada em Matemática. Professora da Secretaria do Estado do Rio Grande do Sul. Rio Grande do Sul, Brasil. ✉ barbaraelisa13@hotmail.com https://orcid.org/0000-0002-5686-0005

[2] Doutora em Ensino de Ciências e Matemática. Professora do Programa de Pós-Graduação em Ensino de Ciências e Matemática da Universidade Luterana do Brasil (ULBRA). Rio Grande do Sul, Brasil. ✉ clarissa.olgin@yahoo.com.br https://orcid.org/0000-0001-5560-9276

Recebido em 21/01/2021 | Aceito em 30/03/2021 | Publicado em 23/05/2021

concluded that the elaboration of contextualized activities can contribute to the development of the content of matrices and the use of electronic spreadsheets, as a technological resource, can be a facilitator for the teaching and learning process of students from high school.

***Keywords**:* Mathematics Curriculum. High School. Matrices. Cryptography. Electronic Spreadsheets.

Construcción de conocimiento matemático utilizando el tema de la criptografía para la Escuela Secundaria

***Resumen*:** Con el uso intensivo de tecnologías digitales por parte de la sociedad, la privacidad y seguridad de la información transmitida entre individuos a través de Internet se vuelve cada vez más necesaria. Es en este escenario donde el cifrado se vuelve fundamental, ya que permite que los datos se compartan de forma segura por estos medios. Así, se entiende que este tema tiene potencial para ser explorado en el aula, especialmente en la enseñanza de las matemáticas. El objetivo de este artículo es presentar los aportes de una secuencia didáctica con el uso de hojas de cálculo que involucran el tema criptografía y el contenido de matrices de secundaria. Se trata de una investigación matemática, desarrollada con seis estudiantes del 3er año de secundaria, de una escuela pública, en el estado de Rio Grande do Sul (Brasil). Los datos se obtuvieron mediante la aplicación de cuestionarios, registros escritos y archivos guardados en hojas de cálculo electrónicas, lo que permitió analizar la propuesta didáctica. A partir de estos registros, parece que es posible trabajar el contenido de las matrices de forma contextualizada y combinada con el uso de hojas de cálculo electrónicas. A través de este estudio se concluye que la elaboración de actividades contextualizadas puede contribuir al desarrollo del contenido de las matrices e, incluso, el uso de hojas de cálculo electrónicas, como recurso tecnológico, puede ser un facilitador para el proceso de enseñanza y aprendizaje de los estudiantes de la Escuela Secundaria.

Palabras clave: Currículo de Matemáticas. Escuela Secundaria. Matrices. Criptografía. Hojas de Cálculo.

Introdução

Os documentos curriculares nacionais salientam a importância de abordar os conteúdos matemáticos de forma contextualizada, buscando contribuir para a formação dos estudantes, assim como demonstrar a aplicabilidade dos mesmos (BRASIL, 1997; 1998; 2000; 2006; 2018; 2019). À vista disso, os Temas Contemporâneos Transversais (TCTs), apresentados pela Base Nacional Comum Curricular (BNCC) trazem temáticas relevantes que devem ser abordadas ao longo do currículo escolar (BRASIL, 2019). Nessa linha, Olgin (2015) contribui com sua pesquisa sobre Temas de Interesse que abordam assuntos (temas) que permitem o desenvolvimento de conteúdos matemáticos. Assim, a pesquisadora os classifica em oito temáticas, destacando-se neste artigo a temática Contemporaneidade, a qual abrange questões oriundas da vida na sociedade, como o tema criptografia.

Segundo Carneiro (2015, p. 3), a criptografia consiste em “estudar 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”. O avanço das tecnologias torna a criptografia indispensável, pois necessita-se cada vez mais de privacidade e seguridade na troca de informações por meios tecnológicos (URGÉLLES, 2018). Além do mais, a criptografia viabiliza a aplicabilidade de conteúdos matemáticos de maneira contextualizada, já que se encontra no cotidiano da sociedade.

Diante do exposto, o presente artigo tem como objetivo apresentar as contribuições de uma sequência didática com a utilização de planilhas eletrônicas envolvendo o tema criptografia e o conteúdo de matrizes do Ensino Médio. Assim, deseja-se produzir o conhecimento por meio de tecnologias digitais e, com base na temática Contemporaneidade apresentada por Olgin (2015), entende-se que a criptografia pode ser trabalhada com os estudantes do Ensino Médio, uma vez que apresenta a aplicabilidade dos conteúdos matemáticos e os contextualiza. A sequência foi aplicada de forma remota com estudantes do 3° ano do Ensino Médio, de uma escola pública do munícipio de Montenegro/RS.

O ensino de matemática por meio de temáticas contemporâneas e de interesse

Na tentativa de reestruturar o sistema de ensino e viabilizar o trabalho com questões sociais, já eram recomendados, pelos Parâmetros Curriculares Nacionais (PCN), o trabalho com Temas Transversais (BRASIL, 1997). Trata-se de temas que buscam debater assuntos relativos à construção social de forma transversal nas disciplinas escolares (MONTEIRO; POMPEU JUNIOR, 2001). Complementa Barbosa (2013, p.10), que os temas transversais visam “garantir a interdisciplinaridade no ensino/aprendizagem e de possibilitar que o aprendiz torne significativo o que aprende”.

Em 1998, buscando práticas escolares interdisciplinares, as Diretrizes Curriculares Nacionais para o Ensino Médio estabeleceram a divisão do Currículo em áreas de conhecimento (BRASIL, 1998), tendo como objetivo que os estudantes estabelecessem relações entre os conteúdos das distintas áreas constituintes do saber. Fato esse destacado pelos Parâmetros Curriculares Nacionais do Ensino Médio (PCNEM) que mencionavam a importância do desenvolvimento dos conteúdos de forma interdisciplinar e por meio de temas transversais (BRASIL, 2000; ÁLVAREZ *et al*., 2002). Ainda, as Orientações Curriculares para o Ensino Médio ressaltam a importância da contextualização

como uma forma de desenvolver os conhecimentos escolares (BRASIL, 2006).

Segundo a Base Nacional Comum Curricular (BNCC) é dever dos sistemas e redes de ensino "[...] incorporar aos currículos e às propostas pedagógicas a abordagem de temas contemporâneos que afetam a vida humana em escala local, regional e global, preferencialmente de forma transversal e integradora" (BRASIL, 2018, p. 19). Para a normativa, as escolas e instituições de ensino devem planejar propostas pedagógicas que reflitam "[...] as necessidades, possibilidades e os interesses dos estudantes, assim como suas identidades linguísticas, étnicas e culturais" (BRASIL, 2018, p. 15). Em concordância Viçosa *et al* (2020, p. 182) destacam que "a transversalidade pode ser compreendida como um conjunto indissociável e indispensável no desenvolvimento de habilidades, competências e valores na formação do educando".

A preocupação com a relação dos estudantes com o ensino é destacada nos documentos curriculares nacionais mencionados. Com esse intuito, a BNCC apresenta os Temas Contemporâneos Transversais (TCTs) que:

> buscam uma contextualização do que é ensinado, trazendo temas que sejam de interesse dos estudantes e de relevância para seu desenvolvimento como cidadão. O grande objetivo é que o estudante não termine sua educação formal tendo visto apenas conteúdos abstratos e descontextualizados, mas que também reconheça e aprenda sobre temas que são relevantes para sua atuação na sociedade (BRASIL, 2019, p. 7).

Os TCTs abordam assuntos que refletem o cotidiano vivenciado pela comunidade escolar, temas da contemporaneidade e que podem ser trabalhados de forma transversal entre as áreas de conhecimento (BRASIL, 2019; VIÇOSA *et al.*, 2020). Por desenvolverem habilidades relacionadas aos componentes curriculares, os TCTs são considerados conteúdos essenciais para a Educação Básica, sendo divididos em seis macroáreas temáticas[3] que englobam quinze Temas Contemporâneos[4].

O trabalho de Olgin (2015), referente aos Temas de Interesse, vai ao encontro das propostas de contextualização dos conteúdos de Matemática do Ensino Médio. Os temas abordados viabilizam aos estudantes "[...] valores sociais, culturais, políticos, econômicos, de forma a atender as necessidades e objetivos dos sujeitos envolvidos nessa relação, que

[3] As macroàreas temáticas dos TCTs são Meio Ambiente, Economia, Saúde, Cidadania e Civismo, Multiculturalismo e Ciência e Tecnologia (BRASIL, 2019).
[4] Os Temas Contemporâneos abordados nas macroàreas dos TCTs são Ciência e Tecnologia, Direitos da Criança e do Adolescente, Diversidade Cultural, Educação Alimentar e Nutricional, Educação Ambiental, Educação para a valorização do multiculturalismo nas matrizes históricas e culturais Brasileiras, Educação em Direitos Humanos, Educação Financeira, Educação Fiscal, Trabalho, Educação para o Consumo, Educação para o Trânsito, Processo de envelhecimento, respeito e valorização do Idoso, Saúde e Vida Familiar e Social (BRASIL, 2019).

permitam a formar um cidadão atuante e comprometido" (OLGIN, 2015, p. 65). São classificados em oito temáticas[5] de forma a promover no Currículo de Matemática "[...] uma Educação Crítica, transformadora, reflexiva, rica em contextos, permitindo ao estudante envolver-se em cada assunto de forma a revisar, aprofundar, exercitar e estudar os conteúdos da Área da Matemática" (OLGIN, 2015, p 130).

Para esta pesquisa utilizou-se a temática Contemporaneidade, na qual Olgin (2015) sugere a criptografia como um tema a ser trabalhado, uma vez que possibilita o desenvolvimento dos conteúdos matemáticos de aritmética, aritmética modular, função linear, função quadrática, função exponencial, função logarítmica, matrizes e polinômios.

Entre as competências gerais da BNCC, a quinta refere-se a

> 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, 2018, p. 9).

Portanto, percebe-se que o trabalho com temáticas é indicado para o Currículo de Matemática do Ensino Médio e um tema que pode ser explorado é a criptografia por meio de uma sequência de atividades que explorem sua história e os conteúdos matemáticos.

Criptografia: um breve histórico

A palavra criptografia pode ser traduzida como uma escrita secreta (CARNEIRO, 2017), referindo-se à arte ou ciência de escrever em código, sendo considerada tão antiga quanto a própria escrita (URGELLÉS, 2018). Era utilizada pelos egípcios e romanos, em seu sistema de escrita hieroglífica, para transmitir seus planos de batalha (TAMAROZZI, 2001). O desenvolvimento de métodos para a ocultação do conteúdo de mensagens foi primordial para transmiti-las de forma eficientes e seguras, sem que fossem interceptadas e, assim, revelado seu conteúdo. Com esse objetivo surgem os códigos, as cifras e as chaves[6] que tornam possível o cenário da criptografia. Via de regra, as guerras impulsionaram a criptografia, uma vez que necessitavam de uma comunicação segura entre seus aliados.

[5] Os Temas de Interesse são classificados em Contemporaneidade, Político-Social, Cultura, Meio Ambiente, Conhecimento Tecnológico, Saúde, Temáticas Locais e Intramatemática (OLGIN, 2015).
[6] Um *código* é definido com uma substituição de palavras ou frases, já a *cifra* é definida com uma substituição de letras, enquanto a *chave* é o parâmetro utilizado para criptografar uma mensagem (URGELLÉS, 2018).

No século V a.C., os espartanos utilizaram o Citale para transmitir suas mensagens durante a guerra com os atenienses. O aparelho consistia em um bastão de madeira no qual se enrolava tiras de couro ou papel e a mensagem era escrita ao longo do comprimento do bastão. O método criptográfico empregado pelo Citale é a transposição, que se dá pelo arranjo dos caracteres da mensagem (URGELLÉS, 2018).

Um dos primeiros métodos criptográficos de substituição foi desenvolvido pelo grego Políbio (203-120 a.C.), que consiste na substituição das letras da mensagem por outras letras ou símbolos. Na Cifra de Políbio, cada letra era substituída por um par de letras. Já a Cifra de César, desenvolvida no século I a.C., substituía cada letra por outra letra que estava três posições avançadas (URGELLÉS, 2018). Os métodos criptográficos de substituição que utilizam cifras monoalfabética[7], como as mencionadas, eram muitos simples e facilmente decifradas pelos criptoanalistas por meio da análise de frequência[8].

O método criptográfico de substituição de cifras polialfabéticas[9] foi desenvolvido por Leon Battista Alberti ao criptografar uma mensagem utilizando dois alfabetos cifrados. Apesar disso, a Cifra de Vigenère, idealizada pelo francês Blaise de Vigenère no século XVI, tornou-se a mais famosa cifra utilizando este método. Consiste em criptografar uma mensagem a partir de um palavra-chave e 26 alfabetos criptografados (SINGH, 2003; URGELLÉS, 2018). No século XVII, a Cifra de Gronsfeld, idealizada pelo holandês Josse Maximilaan Bronckhorst, utilizava apenas 10 alfabetos criptografados e, como palavra-chave, os algarismos de 0 a 9. Já, no século XIX, o barão britânico Lyron Playfair e Sir Charles Wheatstone elaboraram uma variação da Cifra de Políbio, a chamada Cifra de Playfair. Trata-se de uma cifra de substituição de cada par de letras por outro par (SINGH, 2003; URGELLÉS, 2018).

Durante a Primeira Guerra Mundial, os alemães utilizaram a Cifra ADFGVX para codificar suas mensagens com a combinação dos métodos de substituição e transposição (SINGH, 2003; URGELLÉS, 2018). Em 1923, a invenção de Arthur Scherbius foi a grande aliada da Alemanha nazista na Segunda Guerra Mundial. Essa invenção, denominada Máquina Enigma, era um dispositivo eletromecânico que realizava a cifragem de mensagens a partir de manuais. Mas, em 1939, na fazenda de Bletchley Park, uma equipe de criptoanalista, entre eles Alan Turing, decifraram o quebra-cabeça da Máquina Enigma

[7] As cifras monoalfabética empregam apenas um alfabeto para cifrar uma mensagem. Logo, cada letra cifrada terá apenas uma única atribuição (URGELLÉS, 2018).
[8] Análise na qual avalia a frequência com que a letra ou símbolo aparece na mensagem e relaciona com a frequência com que as letras são empregadas no alfabeto correspondente ao idioma utilizado na criptografia (URGELLÉS, 2018).
[9] As cifras polialfabéticas empregam mais de um alfabeto para cifrar uma mensagem. Logo, cada letra cifrada poderá ter mais de uma atribuição (URGELLÉS, 2018).

(SINGH, 2003; URGELLÉS, 2018). Essa mesma equipe desenvolveu o primeiro protótipo de computador moderno da história, o Colossus.

Buscando outro método de criptografia, o matemático americano Lester S. Hill desenvolveu um sistema que empregava uma combinação de aritmética modular e álgebra linear, com o emprego de matrizes. Todavia, é a computação moderna que representa um grande avanço para a criptografia. A linguagem binária, empregada nos computadores, realizava com mais agilidade e rapidez o mesmo trabalho que uma máquina de criptografia convencional. Conforme Urgellés (2018), para manter seguras as mensagens enviadas pelos computadores, em 1970, foi desenvolvida uma das primeiras criptografias projetadas para os computadores, conhecida como Lucifer.

O algoritmo de chave pública[10] foi teorizado por Whitfield Diffie. Contudo, em 1977, Ron Rivest, Adi Shamir e Len Adelman apresentam o algoritmo RSA. Trata-se de um algoritmo de chave pública baseado nas propriedades dos números primos e utilizado até hoje (BENATTI; BENATTI, 2019). Porém, os estudos relativos à computação quântica podem representar um colapso para a criptografia que se conhece. Uma vez que um computador quântico poderá processar uma informação com muito mais agilidade que um computador convencional por meio da superposição de estados[11]. Os estudos de Chales Henry Bennett e Gilles Brassarde, em 1984, idealizaram um sistema de criptografia baseado na transmissão de fótons polarizados, mostrando que a criptografia quântica é possível (URGELLÉS, 2018).

Para Rodrigues e Sá (2019, p. 259) “a criptografia pode ser entendida como um tema gerador de investigação matemática e facilitador de ensino, por se apresentar no cotidiano dos estudantes, mesmo que, muitas vezes, de forma implícita, e pode possibilitar um envolvimento construtivo e prazeroso”. Dessa forma, percebe-se que é possível utilizar tanto atividades históricas, mostrando o desenvolvimento dessa temática ao longo da história na elaboração da sequência didática proposta, quanto relacionar a mesma aos conteúdos matemáticos trabalhados no Ensino Médio.

Metodologia

A pesquisa possui uma abordagem qualitativa, a qual visa descrever o significado

[10] Em um algoritmo de chave pública os remetentes têm acesso a uma chave de criptografia divulgada e cada receptor possui sua própria chave pública (URGELLÉS, 2018).
[11] Se diz quando uma partícula pode assumir, ao mesmo tempo, mais de uma posição ou possui simultaneamente diferentes quantidades de energia (URGELLÉS, 2018).

do resultado das informações obtidas através de questionários, registros escritos e arquivos das atividades realizadas pelos participantes, sem a mensuração quantitativa. Para tanto, se faz necessário uma análise e reflexão mais profunda dos dados obtidos para o entendimento do objeto estudado (BOGDAN; BIKLEN, 1994). Também, busca-se descrever, por meio de uma análise descritiva, os dados obtidos na aplicação da pesquisa como forma de compreensão e dando significado ao objeto estudado (BOGDAN; BIKLEN, 1994).

Visando potencializar o processo de ensino e aprendizagem dos conteúdos matemáticos, buscou-se elaborar uma sequência didática que permitisse utilizar os recursos tecnológicos aliado ao tema criptografia para o desenvolvimento do conteúdo de matrizes, como proposto pelos documentos curriculares nacionais (BRASIL, 2018; 2019).

Com esse intuito, a pesquisa foi desenvolvida em cinco momentos descritos a seguir: O primeiro foi o estudo sobre pesquisas com temáticas no Ensino de Matemática, na qual foram investigado os documentos educacionais brasileiros e a pesquisa de Olgin (2015) quanto ao trabalho com temáticas no Currículo de Matemática do Ensino Médio. O momento seguinte foi a pesquisa sobre o conteúdo de matrizes e sua relação com o tema criptografia, bem com um levantamento histórico sobre o tema. O terceiro momento foi a elaboração de atividades que explorassem as cifras histórias, assim como códigos com o conteúdo de matrizes aliado ao tema, com a utilização de planilhas eletrônicas. O momento seguinte foi a aplicação das atividades com 6 alunos do 3° ano do Ensino Médio de uma escola da rede pública do munícipio de Montenegro/RS, de forma remota por meio da plataforma Moodle[12] e grupo no *Whatsapp*. E, no quinto momento, foi realizada a análise dos dados obtidos a partir dos questionários aplicados, registros escritos e arquivos salvos no *software* Excel enviados na plataforma Moodle pelos participantes.

Atividades com o conteúdo de matrizes aliado ao tema criptografia

Para aplicação da sequência didática com os estudantes do 3° ano do Ensino Médio, foram organizados encontros, conforme apresentado no Quadro 1.

[12] Pesquisa aprovada pelo Comitê de Ética sob CAAE 20057119.1.0000.5349.

Quadro 1: Encontros para aplicação da sequência didática

Semana	Recurso utilizado para os encontros	Atividade
Primeira	Videoconferência	Apresentação, cadastramento na plataforma Moodle e aplicação do questionário inicial.
Segunda	Plataforma Moodle	Apresentação em PPT da história em quadrinhos envolvendo o tema criptografia e duas atividades da Cifra de Vigenère.
Terceira	Plataforma Moodle	Duas atividades da Cifra Playfair e duas atividades da Cifra ADFGVX.
Quarta	Plataforma Moodle	Duas atividades da Cifra de Hill.
Quinta	Plataforma Moodle	Duas atividades da Cifra MKO.
Sexta	Videoconferência	Aplicação do questionário final e encerramento.

Fonte: Elaborado pelas Autoras

A criptografia é um conhecimento que foi historicamente construído e que vai ao encontro das competências gerais da BNCC, que busca entender e explicar a realidade por meio desses conhecimentos (BRASIL, 2018). Entende-se, dessa forma, que a criptografia vem para enriquecer o ensino de matrizes no Ensino Médio, uma vez que se percebe uma bagagem histórica que traz vestígios desde os egípcios e romanos (TAMAROZZI, 2001). Buscando explorar cifras históricas, foram elaboradas atividades envolvendo as cifras apresentadas no Quadro 2.

Quadro 2: Atividades de cifras históricas

Atividade	Objetivos
Cifra ADFGVX	Conhecer e aplicar os procedimentos utilizados para codificar e decodificar utilizando a Cifra ADFGVX.
Cifra de Hill	Conhecer e aplicar os procedimentos utilizados para codificar e decodificar utilizando a Cifra de Hill.
Cifra de Playfair	Conhecer e aplicar os procedimentos utilizados para codificar e decodificar utilizando a Cifra de Playfair.
Cifra de Vigenère	Conhecer e aplicar os procedimentos utilizados para codificar e decodificar utilizando a Cifra de Vigenère.

Fonte: Elaborado pelas Autoras

Ainda, foram desenvolvidas atividades que visam à contextualização do conteúdo de matrizes no Ensino Médio, aliado à utilização de tecnologias digitais. Isso porque, de acordo com a BNCC, os estudantes devem compreender e utilizar as tecnologias digitais,

buscando produzir conhecimentos, bem como solucionar problemas (BRASIL, 2018). De acordo com Rodrigues e Sá (2019), utilizar-se de abordagens que remetem a temas que estão envolvidos com tecnologias é uma estratégia de aproximar os estudantes aos conceitos matemáticos. Com esse intuito, as atividades elaboradas relacionam as matrizes e a criptografia com a exploração dos recursos das planilhas eletrônicas do *software* Excel, uma vez que esse programa permite a realização dos cálculos envolvendo matrizes. As atividades da Cifra MKO[13] são apresentadas no Quadro 3.

Quadro 3: Atividades relacionando o conteúdo de matrizes e a Criptografia da Cifra MKO

Atividade	**Objetivos**
Codificando com adição de matrizes	Atividade que explora as operações de adição e matriz inversa.
Codificando com subtração de matrizes	Atividade que explora as operações de subtração e matriz inversa.
Codificando com multiplicação de matrizes	Atividade que explora as operações de multiplicação e matriz inversa.
Codificando com multiplicação por escalar e adição de matrizes	Atividade que explora as operações de adição, multiplicação por escalar e matriz inversa.
Codificando com multiplicação por escalar e subtração de matrizes	Atividade que explora as operações de subtração, multiplicação por escalar e matriz inversa.

Fonte: Elaborado pelas Autoras

A seguir, são apresentadas as atividades elaboradas a partir da Cifra de Playfair e da Cifra MKO, que aborda a parte histórica e explora o conteúdo de matrizes, respectivamente.

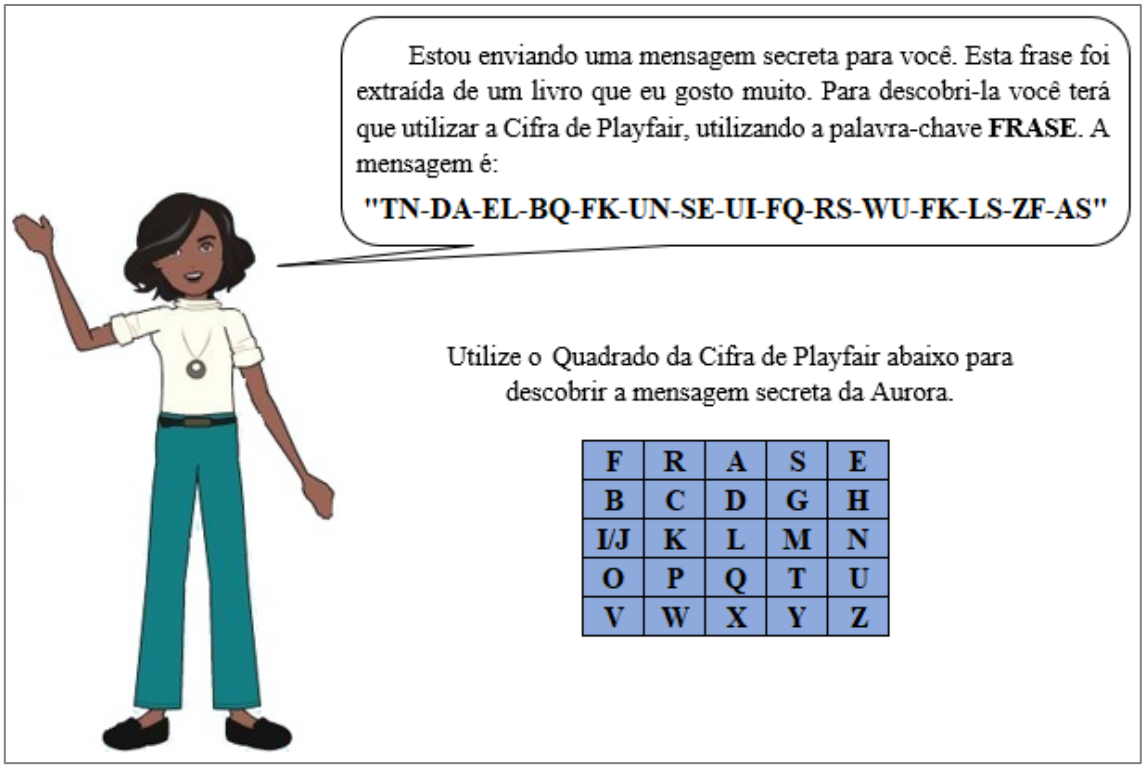
A Cifra de Playfair é composta por um quadro de 5 colunas por 5 linhas, no qual se distribui as letras do alfabeto iniciando-se por uma palavra-chave, sem letras repetidas, e combinando duas letras, a critério (URGÉLLES, 2018). A decodificação de uma mensagem com a utilização desta cifra depende da posição em que as letras do par se encontram no quadro, tendo os seguintes casos: se as letras do par se encontram na mesma linha no quadro, substitui-se pelas letras que estão à esquerda delas; quando se encontram no final da linha, substitui-se pelas letras do início da mesma e vice e versa; ao estarem na mesma coluna, substitui-se pelas letras que se encontram acima das letras do par; se estiverem no final da coluna, substitui-se pelas letras no início da coluna e vice e versa; e no caso das

[13] A Cifra MKO possui um alfabeto codificador e decodificador (Figura 3), sendo elaborada pela primeira autora deste artigo para a sua dissertação de mestrado.

letras do par não estarem nem na mesma linha, nem na mesma coluna, deve-se substituir pela letra de encontro entre o par, de forma que se encontre na mesma linha da letra em questão e na coluna da outra.

Apresenta-se a seguir, uma atividade desenvolvida a partir da Cifra de Playfair (Figura 1).

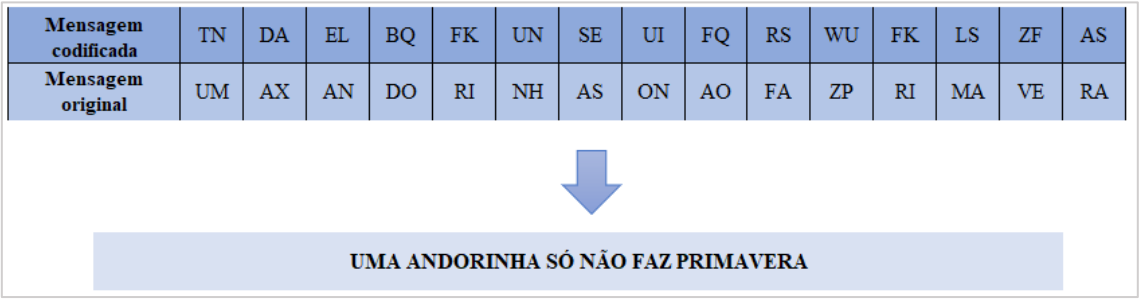
Figura 1: Atividade desenvolvida a partir da Cifra de Playfair



Fonte: Elaborado pelas Autoras

Para a decodificação da mensagem deve-se, inicialmente, agrupar as letras da mesma em pares. Em seguida, com o auxílio do alfabeto, decodifica-se a mensagem de acordo com cada caso (Figura 2).

Figura 2: Decodificação da mensagem



Fonte: Elaborado pelas Autoras

A atividade da Cifra MKO que será apresentada envolve as operações de subtração

e multiplicação por escalar em uma matriz. Para a decodificação da mensagem com a utilização da Cifra, foi elaborado um alfabeto codificador/decodificador (Figura 3).

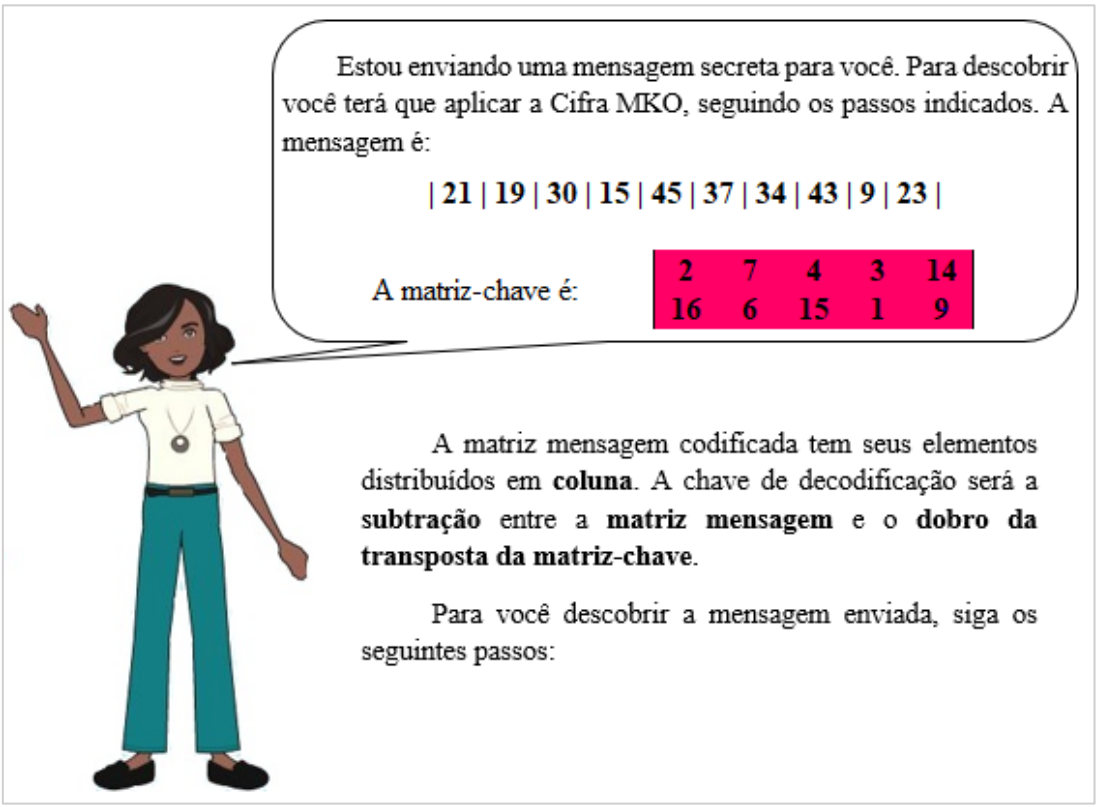
Figura 3: Alfabeto codificador/decodificar da Cifra MKO

A	B	C	D	E	F	G
5	4	7	6	9	8	11
H	**I**	**J**	**K**	**L**	**M**	**N**
10	13	12	15	14	17	16
O	**P**	**Q**	**R**	**S**	**T**	**U**
19	18	21	20	23	22	25
V	**W**	**X**	**Y**	**Z**	**Ç**	*****
24	27	26	29	28	31	30

Fonte: Elaborado pelas Autoras

Essa atividade visa transformar a mensagem em uma matriz de ordem *m*x*n*, de forma que possa ser subtraída do dobro da transposta da matriz-chave (Figura 4).

Figura 4: Atividade da Cifra MKO

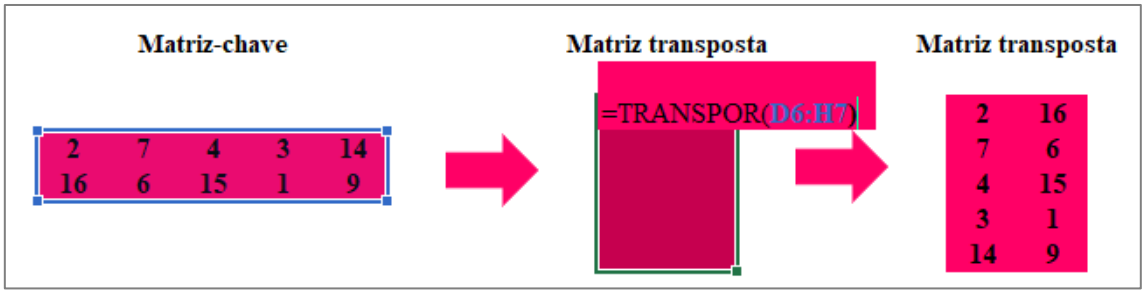


Fonte: Elaborado pelas Autoras

Inicialmente, deve-se descobrir a matriz-chave que operará com a matriz-mensagem. Conforme descrição da atividade, busca-se determinar o dobro da transposta da matriz-chave. Assim, explora-se os comandos das planilhas eletrônicas do *software*

Excel[14] que determinam a transposta de uma matriz e a multiplicação de matriz por um escalar. Para calcular a transposta da matriz, é necessário selecionar a quantidade de células correspondentes a transposta e digitar o sinal de igual seguido do comando "TRANSPOR", selecionando a matriz. Após, aperta-se as teclas *ctrl* + *shift* + *enter* e a matriz transposta é dada (Figura 5).

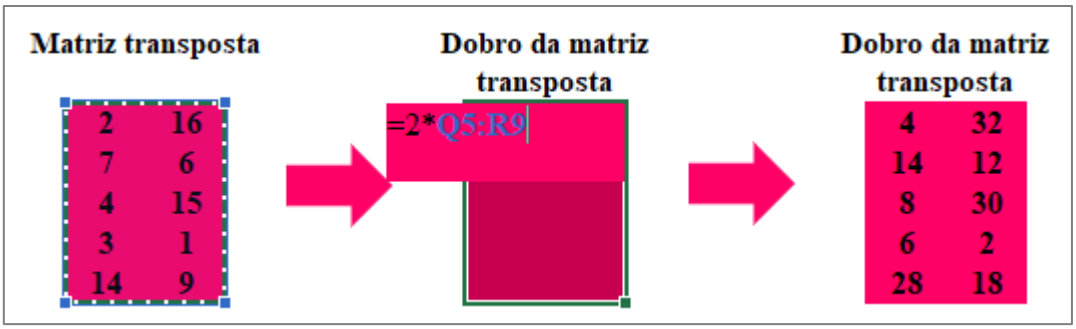
Figura 5: Comandos para determinar a matriz transposta



Fonte: Elaborado pelas Autoras

Para determinar o dobro da matriz transposta, deve-se selecionar a quantidade de células correspondentes ao dobro da matriz transposta e digitar o sinal de igual seguido do algarismo 2, o sinal de multiplicação nas planilhas eletrônicas (asterisco), entre parênteses selecionar a matriz e aperta a tecla *enter* (Figura 6).

Figura 6: Comandos para determinar o dobro da matriz transposta

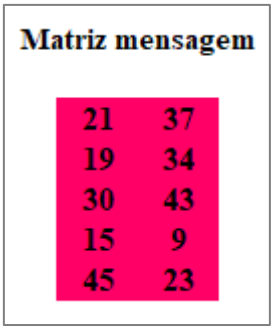


Fonte: Elaborado pelas Autoras

Em seguida, a mensagem enviada deve ser transformada em uma matriz. Ressalta-se que sua ordem deve ser a mesma do dobro da matriz transposta gerada (Figura 7).

[14] Nesta pesquisa foram utilizadas as planilhas eletrônicas do *software* Excel, assim os comandos apresentados referem-se a este *software*.

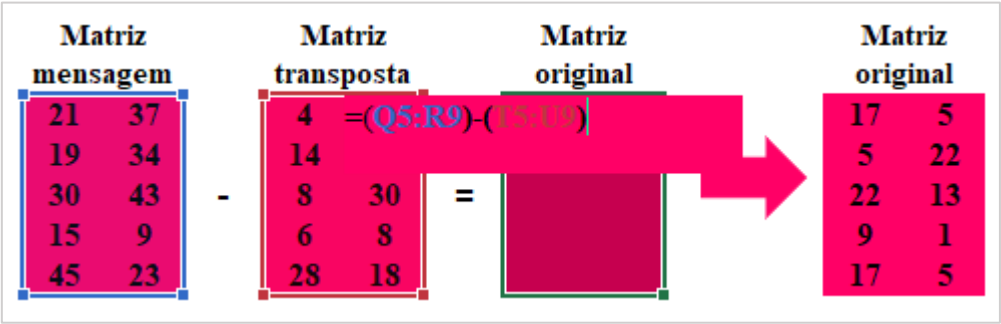
Figura 7: Transformando a mensagem em uma matriz



Fonte: Elaborado pelas Autoras

Agora, para determinar a matriz original, é necessário subtrair da transposta da matriz-chave a matriz mensagem. Lembrando-se que para efetuar a subtração de matriz é necessário que as matrizes sejam de mesma ordem. Então, explora-se o comando da planilha eletrônica que permite determinar a subtração de matrizes. Seleciona-se a quantidade de células correspondente a matriz resultante e digita-se o comando como se apresenta na Figura 8. Após, clica-se nas teclas *ctrl* + *shift* + *enter* e a matriz resultante é obtida.

Figura 8: Comando para determinar a subtração de matrizes



Fonte: Elaborado pelas Autoras

Por último, com o auxílio do alfabeto codificador/decodificador apresentado na Figura 3, decodifica-se a mensagem realizando a correspondência dos elementos da matriz, em colunas, com o alfabeto. Dessa forma, a mensagem decodificada é “MATEMÁTICA”.

As atividades apresentadas evidenciam a possibilidade de criar uma sequência didática que contextualiza a aplicação do conteúdo de matrizes com o tema criptografia e a utilização de planilhas eletrônicas.

Descrição e análise da sequência didática

A sequência foi aplicada remotamente, via plataforma Moodle, com 6 estudantes do 3° ano do Ensino Médio, da Escola Estadual Técnica São João Batista, em Montenegro/RS.

Para a análise dos resultados os estudantes, foram denominados: Estudante A, Estudante B, Estudante C, Estudante D, Estudante E e Estudante F.

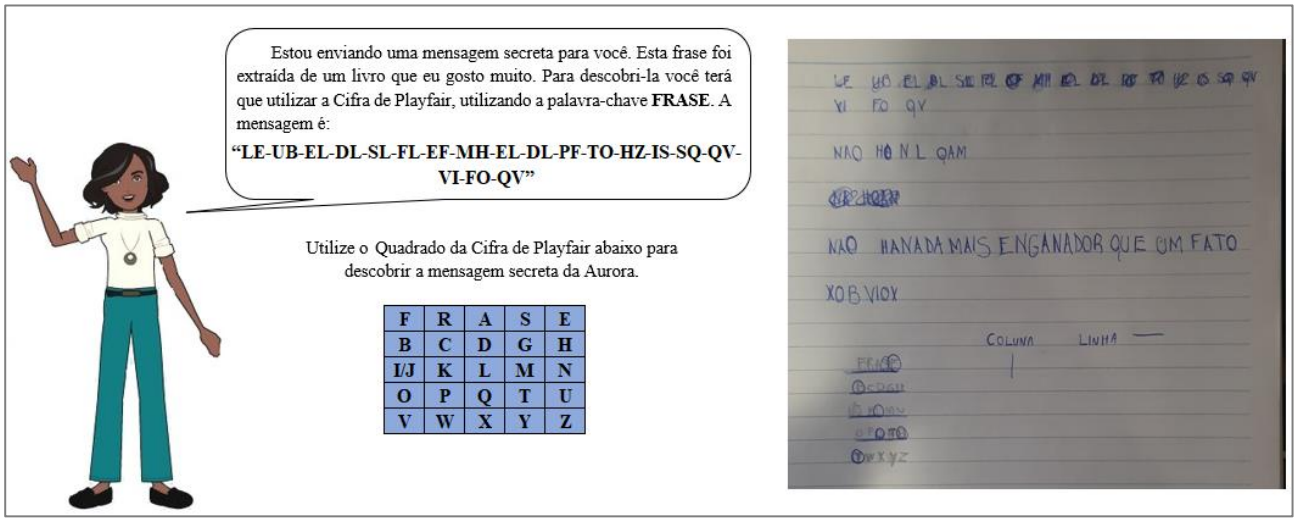
O grupo de estudantes que participou da pesquisa têm entre 17 e 18 anos, com apenas um deles exercendo atividade profissional. Todos tiveram contato com o conteúdo de matrizes no último ano letivo de 2019. Em relação ao tema criptografia, os seis estudantes tinham conhecimento do que se tratava o assunto, mas apenas dois tiveram contato durante o Ensino Fundamental ou Ensino Médio, nas disciplinas de Matemática e/ou Língua Portuguesa e um estudante durante um Curso de Informática. Em relação à utilização das planilhas eletrônicas, quatro estudantes tiveram contato, mas apenas dois responderam ter noção de operações no *software*.

Salienta-se que todas as atividades foram elaboradas no *software* Excel. Ainda, para o desenvolvimento da resolução das Cifras de Hill e MKO, que podem explorar os comandos da planilha eletrônica foi exemplificado aos participantes como utilizar os comandos das planilhas para a resolução de atividades envolvendo o cálculo de matrizes.

Conforme as competências da BNCC, os conhecimentos historicamente construídos devem ser desenvolvidos com os estudantes em sala de aula. Assim, as atividades envolvendo as cifras históricas visam mostrar a importância desses conhecimentos ao longo dos séculos.

Para solucionar a atividade da Cifra de Playfair, o estudante A utilizou o papel para escrever a mensagem codificada e realizar a decodificação da mensagem, conforme a Figura 9.

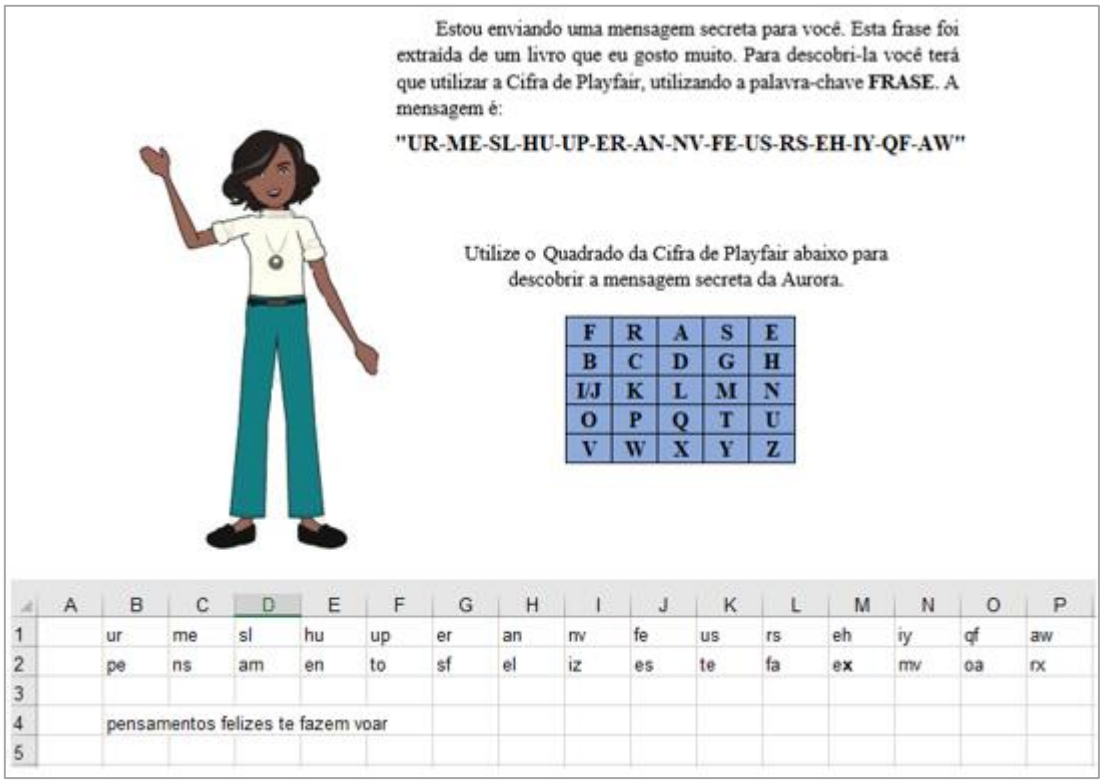
Figura 9: Resolução da atividade de Cifra de Playfair do estudante A



Fonte: Registro escrito do Estudante A

Já o estudante B utilizou as planilhas eletrônicas para encontrar a mensagem decodificada (Figura 10). Os estudantes realizaram a atividade, conforme a análise *a priori* da pesquisadora, porém o estudante A foi o único que não utilizou as planilhas eletrônicas para encontrar a mensagem codificada.

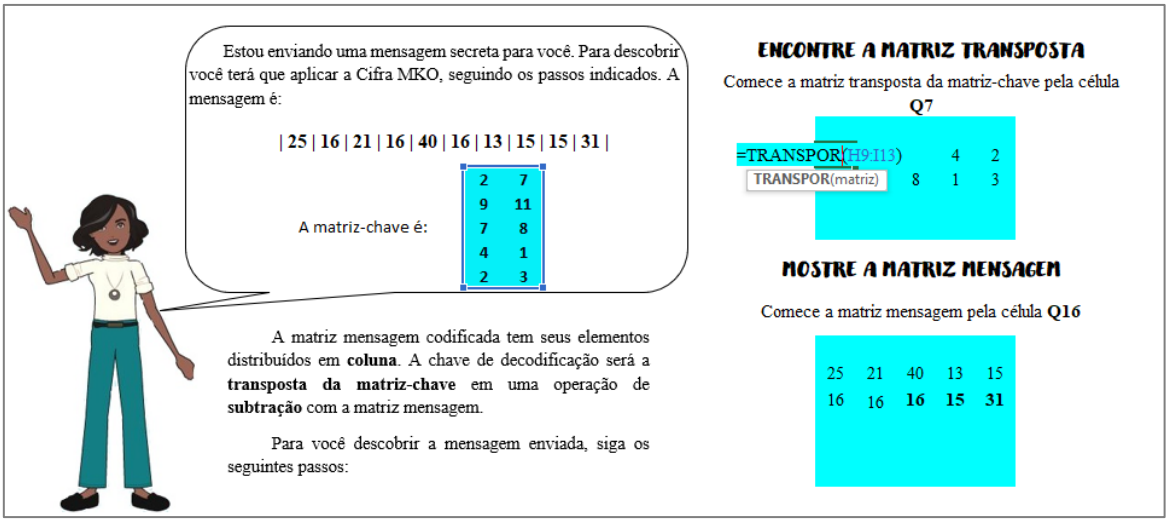
Figura 10: Resolução da atividade da Cifra de Playfair do estudante B



Fonte: Arquivo da planilha eletrônica do Estudante B

A pesquisa de Olgin (2015) explora o tema criptografia com a contextualização do conteúdo de matrizes, isso porque é possível elaborar atividades que relacionam as operações de matrizes com cifras. Em relação às atividades da CIFRA MKO, observa-se que os estudantes C e D exploraram a operação de *transpor* nas planilhas eletrônicas. Como exemplo, apresenta-se a resolução do Estudante C, na Figura 11. Os outros quatro estudantes realizaram de forma manual a transposição da matriz-chave.

Figura 11: Resolução da matriz transposta pelo estudante C



Fonte: Arquivo da planilha eletrônica do Estudante C

Observando a figura, percebe-se que o estudante selecionou o número de células adequadas para utilizar a função transpor da planilha eletrônica, obtendo, assim, a matriz transposta.

No que se refere as operações de adição ou subtração entre matrizes, os estudantes B e C exploraram os comandos para os cálculos, mas observa-se que eles se confundiram ao efetuar as operações, pois realizaram a subtração da transposta da matriz-chave pela matriz mensagem, quando deveriam ter feito o oposto para chegar na matriz original. Na Figura 12, apresenta-se a resolução do Estudante B.

Figura 12: Resolução da subtração de matrizes pelo Estudante B

Matriz Transposta			Matriz Mensagem			Matriz Original	
4	32		21	37		-17	-5
14	12	menos	19	34		-5	-22
8	30		30	43	igual	-22	-13
6	2		15	9		-9	-7
28	18		50	23		-22	-5

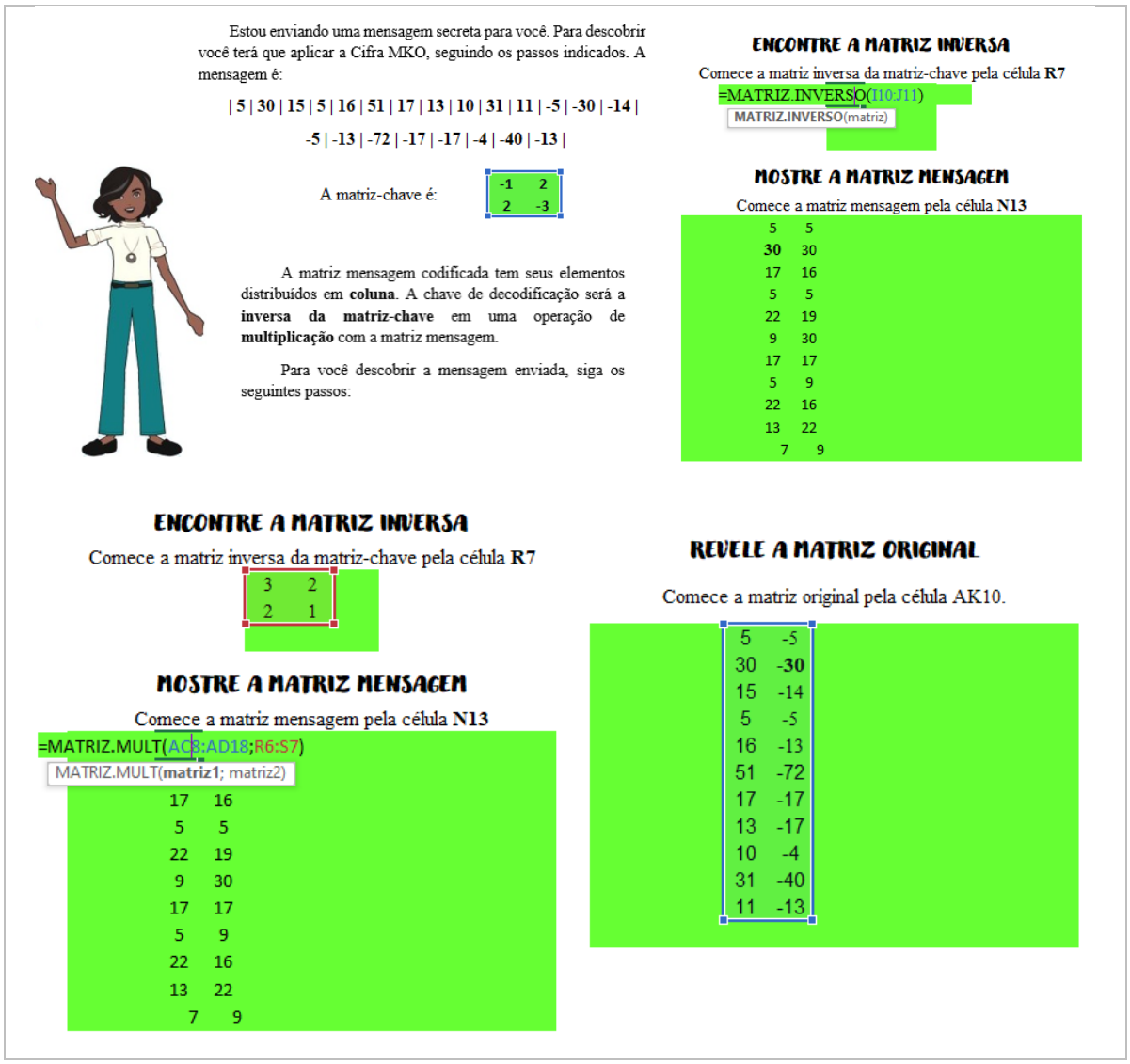
Fonte: Arquivo da planilha eletrônica do Estudante B

O equívoco nas atividades de adição e subtração pelos estudantes B e C podem ter ocorrido, porque os estudantes não interpretaram adequadamente o enunciado das atividades e, também, não analisaram que o alfabeto codificador/decodificar apresenta apenas valores positivos, sendo assim o resultado não poderia ser expressado por valores negativos.

Quanto às atividades da CIFRA MKO, que envolviam as operações de inversa e

multiplicação entre matrizes, os estudantes A, C e D utilizaram os comandos das planilhas eletrônicas para realizar as operações. Na Figura 13, apresenta-se a resolução do estudante B.

Figura 13: Resolução da matriz inversa e da multiplicação entre matrizes pelo estudante B



Fonte: Arquivo da planilha eletrônica do Estudante B

De acordo com os dados informados no questionário final pelos seis estudantes que participaram da pesquisa, tanto as atividades quanto o tema criptografia contribuíram para o entendimento do conteúdo de matrizes. A opção por selecionar as planilhas eletrônicas do Excel se dá pela determinação dos cálculos de matrizes, uma vez que, ao utilizar esse recurso, os conceitos desse conteúdo devem estar bem estruturados como, por exemplo, para realizar o cálculo da matriz transposta de ordem 2x3, o estudante precisa saber que a transposta dessa matriz é uma matriz de ordem 3x2, isso permitirá que sejam selecionadas a quantidade de células na planilha que corresponderá as linhas e as colunas da matriz

transposta. Ainda, ao utilizar esse recurso, oportuniza ao estudante do Ensino Médio o contato com as tecnologias digitais e suas formas de manuseio. Para os seis estudantes as planilhas eletrônicas auxiliaram no desenvolvimento das atividades, como respondeu o Estudante A: *"Elas nos trazem uma forma mais fácil de resolver algumas das situações em que precisamos multiplicar, ou somar matrizes por exemplo".*

Já quanto à relevância da utilização das planilhas eletrônicas em sala de aula como um recurso facilitador, quatro alunos foram favoráveis, um contrário e outo imparcial. O Estudante C traz a seguinte fala: "*Acho que não é necessário, até porque os alunos estão lá para aprender a fazer contas matemáticas. Como as planilhas já resolvem os exercícios, então não tem necessidade*".

Enquanto, o Estudante A se apresenta imparcial:

> "*Essa é uma questão da qual não tenho total certeza, ela facilita bastante na hora da resolução das atividades, porém ela não deve ser utilizada em todos os momentos, pois assim nos tornamos dependentes da tecnologia e muitas das vezes em momentos em que iremos precisar do conhecimento, podemos não ter o mesmo pelo fato de usufruir em 100% do tempo destes meios."*

E, por fim, em relação às contribuições da utilização da criptografia e das planilhas eletrônicas quanto ao entendimento do conteúdo de matrizes, cinco estudantes confirmam ter contribuído, como afirma o Estudante F: *"Sim, pois, percebi que as matrizes podem ser representadas por tabelas, e que, quando usamos o Excel, podemos realizar operações com matrizes de forma muito mais fácil"*.

Portanto, conforme as indicações da BNCC, considera-se importante explorar os recursos tecnológicos nas atividades em sala de aula, bem como diferentes Temas Contemporâneos Transversais para o desenvolvimento dos conteúdos matemáticos do Ensino Médio. Mas, cabe ressaltar que as atividades devem ser planejadas, a fim de atingir os objetivos didáticos propostos. Assim, as atividades elaboradas para a sequência didática apresentada são exemplos de que é possível trabalhar o conteúdo de matrizes de forma contextualizada e aliada à utilização de planilhas eletrônicas.

Considerações Finais

A contextualização dos conteúdos matemáticos é abordada em diversos documentos curriculares brasileiros (BRASIL, 1998; 2000; 2006; 2018), e, para tanto, a BNCC traz os Temas Contemporâneos Transversais (BRASIL, 2019). Os Temas de Interesse apresentados na pesquisa de Olgin (2015) vai ao encontro do que é exposto nos

TCT's tornando possível relacionar o conteúdo de matrizes ao tema criptografia. Assim, atividades didáticas que englobam o tema podem ser utilizadas como um recurso potencializador pelos professores durante o processo de ensino e aprendizagem, uma vez que se busca relacionar a teoria com aplicações do conteúdo matemático.

Ao encontro das competências gerais da BNCC utilizou-se as planilhas eletrônicas do Excel como recurso tecnológico para o desenvolvimento de cálculos de operações com matrizes, mas também com o intuito de oportunizar aos estudantes a utilização de tecnologias digitais em sala de aula.

A partir da análise das atividades resolvidas pelos participantes, percebe-se que para a resolução das atividades da Cifra MKO e Cifra de Hill todos os estudantes utilizaram os recursos das planilhas eletrônicas para os cálculos de matrizes. Entretanto, um aluno optou por não utilizar as planilhas eletrônicas para solucionar as atividades envolvendo as Cifras de Vigenère e Cifra de Playfair, enquanto três não a utilizaram para a Cifra de ADFGVX.

Então, entende-se que, a partir da aplicação da sequência didática desenvolvida com o tema criptografia, em um grupo de estudantes do Ensino Médio, essa temática pode contribuir para o desenvolvimento do conteúdo de matrizes com atividades que possibilitam explorar os conceitos de ordem de matriz, matriz transposta, matriz inversa e operações com matrizes. Ainda, a utilização das planilhas eletrônicas do Excel, como recurso tecnológico, pode ser um facilitador para o processo de ensino e aprendizagem dos estudantes, visto que ao conhecer os conceitos do conteúdo podem obter a solução de forma rápida.

Referências

ÁLVAREZ, M. N. *et al*. **Valores e temas transversais no currículo.** Porto Alegre: Editora Artmed, 2002. Traduzido Daisy Vaz de Moraes.

BARBOSA, L. M. S. **Temas transversais**: como utilizá-los na prática educativa? Curitiba: Editora InterSaberes, 2013.

BENNATI, K. A.; BENATTI, N. C. C. M. **Teoria dos Números**. Curitiba: Editora InterSaberes, 2019.

BOGDAN, R.; BIKLEN, S. **Investigação qualitativa em educação**. Portugal: Porto Editora, 1994.

BRASIL. **Lei nº. 9.394**, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da educação nacional. Brasília: Diário Oficial da União, 23 dez. 1996.

BRASIL. Secretária de Educação Fundamental. **Parâmetros Curriculares Nacionais**:

apresentação dos temas transversais, ética. Brasília: MEC/SEF, 1997.

BRASIL. Conselho Nacional de Educação. **Diretrizes Curriculares Nacionais para o Ensino Médio**. Brasília: MEC, 1998.

BRASIL. Ministério da Educação, Secretária de Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais Ensino Médio**. Brasília: MEC/SEMTEC, 2000.

BRASIL. Secretária de Educação Básica. **Orientações Curriculares para o Ensino Médio**. Brasília: MEC/SEB, 2006.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília: MEC, 2018.

BRASIL. Ministério da Educação. **Temas Contemporâneos Transversais na BNCC**: contexto histórico e pressupostos pedagógicos. Brasília: MEC, 2019.

CARNEIRO, F. J. F. **Criptografia e a Teoria dos Números.** São Paulo: Editora Ciência Moderna, 2015.

MONTEIRO, A.; POMPEU JUNIOR, G. **A Matemática e os temas transversais**. São Paulo: Editora Moderna, 2001.

OLGIN, C. A. **Critérios, possibilidades e desafios para o desenvolvimento de temáticas no Currículo de matemática do Ensino Médio**. 2015. 265 f. Tese (Doutorado em Ensino de Ciências e Matemática), Programa de Pós-graduação em Ensino de Ciências e Matemática, Universidade Luterana do Brasil. Rio Grande do Sul, Canoas, 2015.

RODRIGUES, L. P. O.; SÁ, L. C. Matrizes e criptografia: contribuições de uma atividade sobre o *whatsapp* no Ensino Médio. **REnCiMa**, v. 10, n. 6, p. 255-273, 2019.

SINGH, S. **O Livro dos Códigos: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica**. Rio de Janeiro: Editora Record, 2003.

STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. 4ª edição. São Paulo: Editora Pearson Prenticc Hall, 2008. Traduzido por Daniel Vieira.

TAMAROZZI, A. C. Codificando e decifrando mensagens. **Revista do Professor de Matemática**, n. 45, 2011.

URGELLÉS, J. G. **Matemática y códigos secretos.** Barcelona: Editora RBA Libros, 2018.

VIÇOSA, C. S. C. L. et al. Concepções de licenciados acerca de abordagens transversais no ensino de Ciências. **REnCiMa**, São Paulo, v. 11, n. 7, p. 180-197, nov. 2020.