INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS ANGICAL DO PIAUÍ
CURSO DE LICENCIATURA EM MATEMÁTICA

LUCAS GABRIEL LIMA VIANA

PERSPECTIVA DO ESTUDO DA CRIPTOGRAFIA NO ENSINO DA MATEMÁTICA

ANGICAL DO PIAUÍ

2020

LUCAS GABRIEL LIMA VIANA

PERSPECTIVA DO ESTUDO DA CRIPTOGRAFIA NO ENSINO DA MATEMÁTICA

Trabalho de Conclusão de Curso (artigo) apresentado como exigência parcial para obtenção do diploma do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia do Piauí. Campus Angical .

Orientador: Prof. Me. Edem Assunção Baima Neto.

ANGICAL DO PIAUÍ

2020

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

Viana, Lucas Gabriel Lima

V614p Perspectiva do ensino da criptografia no ensino da matemática / Lucas Gabriel Lima Viana. - 2020.

21 f.: il. color.

Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Instituto Federal do Piauí, Campus Angical, 2020.

Orientador : Prof. Me. Edem Assunção Baima Neto.

1. Criptografia. 2. Análise combinatória. 3. Ensino contextualizado. I.Título.

CDD - 510

Elaborado por Jesselina Soares de Sena CRB 3/1373

LUCAS GABRIEL LIMA VIANA

PERSPECTIVA DO ESTUDO DA CRIPTOGRAFIA NO ENSINO DA MATEMÁTICA

Trabalho de Conclusão de Curso (artigo) apresentado como exigência parcial para obtenção do diploma do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia do Piauí. Campus Angical .

Aprovado em: 23/11/2020.

BANCA EXAMINADORA

_____
Prof. Me. Edem Assunção Baima Neto (Orientador)
Instituto Federal do Piauí (IFPI)

_____
Prof. Me. Juraci Pereira dos Santos
Instituto Federal do Piauí (IFPI)

_____
Prof. Me. Maximiano Freitas Silva
Instituto Federal do Piauí (IFPI)

RESUMO

O presente trabalho trata-se de uma pesquisa sobre a utilização da criptografia como estratégia de ensino para o processo de ensino-aprendizagem na disciplina de matemática em temas de álgebra e análise combinatória, sendo abordados de modo geral na educação básica. A pesquisa teve a seguinte prerrogativa que norteou o rumo do estudo: “Como o ensino contextualizado por meio da utilização da criptografia pode auxiliar no processo de ensino-aprendizagem em temas relacionados à álgebra e análise combinatória?”. Para o estudo desses temas é de suma importância que o aluno tenha noções de matemática básica, para isso é importante a contextualização do ensino com a realidade do discente. Para a realização desta pesquisa teve como objetivo geral: Investigar o ensino contextualizado por meio da utilização da criptografia, como ferramenta metodológica auxiliar no processo de ensino-aprendizagem em temas relacionados à álgebra e análise combinatória. Em relação aos objetivos específicos: Relacionar o contexto da criptografia ao conhecimento algébrico e da analise combinatória ensinado no ensino médio, conforme BNCC; destacar a contribuição da criptografia por meio da sua aplicação que resultou em grandes marcos históricos; identificar a importância da contextualização do ensino da álgebra e análise combinatória envolvendo criptografia, como cifra de César e sistema do código de barras. Em busca de identificar os principais teóricos que tratam sobre o tema, o trabalho constitui como base teórica: Singh (2001), Suitônio (2002) e Tamarozzi (2001). Para a consecução dos objetivos foi realizada uma pesquisa bibliográfica em livros, sites, artigos e monografias que tivessem como tema o ensino da matemática por meio da criptografia. Com os resultados da pesquisa foi possível verificar as contribuições da criptografia para o processo de ensino-aprendizagem em matemática por meio do ensino contextualizado.

Palavras-chave: Criptografia. Análise combinatória. Ensino contextualizado

ABSTRACT

The present work is a research on the use of cryptography as a teaching strategy for the teaching-learning process in the subject of mathematics in themes of algebra and combinatorial analysis, being approached in general in basic education. The research had the following prerogative that guided the course of the study: “How can contextualized teaching through the use of cryptography help in the teaching-learning process on topics related to algebra and combinatorial analysis?”. For the study of these themes it is of utmost importance that the student has basic mathematical

notions, for this it is important to contextualize the teaching with the student's reality. To carry out this research, the general objective was to: Investigate contextualized teaching through the use of cryptography, as an auxiliary methodological tool in the teaching-learning process on topics related to algebra and combinatorial analysis. In relation to specific objectives: Relate the context of cryptography to algebraic knowledge and of combinatorial analysis taught in high school, according to BNCC; highlight the contribution of cryptography through its application, which has resulted in major historical milestones; to identify the importance of contextualizing the teaching of algebra and combinatorial analysis involving cryptography, such as César's cipher and barcode system. In order to identify the main theorists who deal with the theme, the work constitutes the theoretical basis: Singh (2001), Suitônio (2002) and Tamarozzi (2001). To achieve the objectives, a bibliographic search was carried out on books, websites, articles and monographs that had the theme of teaching mathematics through cryptography. With the results of the research it was possible to verify the contributions of cryptography to the teaching-learning process in mathematics through contextualized teaching.

Keywords: Cryptography. Combinatorial analysis. Contextualized teaching.

1 INTRODUÇÃO

A ciência da criptografia surge desde de muito cedo estando presente na escrita dos egípcios e dos romanos que a usufruíram de modo a informar estratégias de batalha (TAMAROZZI, 2001). Vale ressaltar que: “Um dos componentes essenciais da criptografia, [...], ocorreu há cerca de 4000 anos na cidade egípcia [...], onde foram escritas as inscrições hieroglíficas na tumba [...] com vários símbolos incomuns para confundir ou obscurecer o significado das inscrições.” (CYPHER RESEARCH LABORATORIES, 2013). De fato, teve como seus precursores os egípcios que fizeram uso para registrar informações em alguns objetos para confundir ou obscurecer o significado, fazendo isso para que tais informações não chegassem a pessoas não autorizadas.

De acordo Tamarozzi (2001, p.1) “A palavra criptografia tem origem grega (*kripto* = escondida, oculto; *grapho* = grafia) e define a arte ou ciência de escrever mensagens em códigos, de forma que somente pessoas autorizadas possam

decifrá-las.” Essa ciência vem se desenvolvendo no decorrer dos anos de modo a assegurar informações confidenciais.

Para tanto, a criptografia sendo uma ciência tão antiga quanto a escrita teve com o advento de determinadas situações ocorridas que fez com fosse utilizada em diferentes contextos, assim como os romanos fizeram seu uso para finalidades militares, a fim de promover a comunicação em campos de batalhas, no intuito de seus inimigos não descobrissem suas mensagens. Que com o passar do tempo foi “peça chave” na Segunda Guerra Mundial, sendo que as informações obtidas pelos inimigos poderiam resultar em uma enorme fatalidade. Para Silva (2000. p.137):

> A criptografia é tão antiga quanta a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalhas. O mais interessante é que a tecnologia de Criptografia não mudou muito até meados deste século. Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de mensagens. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

Com o intuito de guardar informações restritas, onde somente o destinatário poderia obtê-la, mas que no percurso poderia haver interceptações de terceiros não autorizados. Nesse sentido, a criptografia vem evoluindo, por meio da necessidade de tornar a troca de informações mais segura, desse modo, dificultando para as pessoas não autorizados que buscam decodificar as informações.

Com os avanços da criptografia, durante e após a Segunda Guerra Mundial, houve melhorias no âmbito da vida humana e nos meios de comunicação, que se desenvolvem até hoje, como a invenção de aparelhos que fazem uso de meios criptográficos como: rádio, TV, telégrafo, computadores e *smartphones* que utilizam senhas e apps que realizam transações bancárias, envio de documentos, imagens e vídeos, que também possibilitam troca de informações confidenciais.

O estudo da criptografia em sala de aula pode contribuir nas aulas de matemática, tornando o ensino mais dinâmico, chamando a atenção do aluno e demonstrando a aplicação de conceitos matemáticos, assim ressaltando a importância da matemática tem na vida humana, assim como alguns tópicos discutidos em sala de aula como: matrizes, álgebra, MMC (Mínimo Múltiplo Comum), MDC (Máximo Divisor Comum) e análise combinatória. Para tanto, pode-se ressaltar que o estudo desses conceitos desenvolve-se certas aptidões como: raciocínio

lógico matemático abordado por questões problemas e noções de matemática básica, estudada de forma implícita nesses conteúdos.

A análise combinatória por sua vez “[...] visa desenvolver métodos que permitam contar o número de elementos de um conjunto, sendo estes elementos, *agrupamentos formados sob certas condições*” (HAZZAN. 1993 p. 5), visto que em determinadas situações como a exemplo de descobrir quantas senhas sejam possíveis com apenas 4 dígitos, como também em outras situações o estudo da análise combinatória cumpri tais requisitos.

De uma forma prática e contextualizada com o meio social que o estudante está inserido, pode ser uma alternativa para uma aula diversificada, dessa forma quebrando a rotina das aulas tradicionais de matemática que pouco cativam a atenção do aluno. Segundo Oliveira e Kripka (2011, p. 12).

> Acredita-se que a inclusão de atividades que envolvam conceitos de criptografia pode ajudar a diminuir a existência de aulas mecânicas, onde o professor, através de atividades práticas, poderá mostrar a aplicabilidade dos conceitos trabalhados em sala de aula, relacionando-os a fatos importantes ocorridos na atualidade.

Diante disso o professor pode expor seus conteúdos de maneira que venha a convergir com a realidade do aluno, com a utilização de atividades práticas relacionadas ao seu cotidiano. Podemos assim notar que uma estratégia para o ensino contextualizado, que vise aprimorar os conteúdos vistos não só de maneira algébrica, mas também em suas aplicações. Sendo para Delizoicov (2001, p.133) “[...] É preciso que o problema formulado tenha uma significação para o estudante, de modo a conscientizá-lo de que a sua solução exige um conhecimento que, para ele, é inédito”. Nesse sentido, o estudo da criptografia e suas aplicações podem auxiliar o professor com os assuntos matemáticos relacionados ao cotidiano dos alunos.

O ensino da Matemática, não basta somente sobre a utilização do livro didático, pois nem todos os alunos conseguem assimilar os conteúdos propostos em sala de aula com essa metodologia de ensino. Para isso é importante demonstrar a aplicação dos conteúdos matemáticos que estão presentes na vida do aluno, fazendo seu uso mesmo que de maneira implícita. Para Micotti (1999, p.154).

> A aplicação dos aprendizados em contextos diferentes daqueles em que foram adquiridos exige muito mais que a simples decoração ou a solução mecânica de exercícios: domínio de conceitos, flexibilidade de raciocínio, capacidade de análise e abstração. Essas capacidades

> são necessárias em todas as áreas de estudo, mas a falta delas, em Matemática, chama a atenção.

No estudo da Matemática, não basta somente o domínio de conceitos sem capacidade de perceber onde são aplicados, para Micotti (1999) o ensino aplicado em diferentes contextos contribui para o desenvolvimento na análise e de abstração que podem ser desenvolvidos no estudante em estudos contextualizados em sala de aula, podendo facilitar o processo de ensino aprendizagem.

Alguns tópicos de criptografias podem ser adequados e aplicados em sala de aula, para tanto deve-se moldar tais tópicos para que atinjam os competências e habilidades de ensino que irá distinguir de cada ano/série que se faz a aplicação. Em relação a Transposição Didática temos que para Chevallard (1991, p.39)

> Um conteúdo de saber que tenha sido definido como saber a ensinar, sofre, a partir de então, um conjunto de transformações adaptativas que irão torná-lo apto a ocupar um lugar entre os objetos de ensino. O 'trabalho' que faz de um objeto de saber a ensinar, um objeto de ensino, é chamado de transposição didática.

Segundo o PCN de Matemática, esta possui importante relevância para o desenvolvimento do raciocínio lógico do aluno, possibilitando-o generalizar e prever algumas situações "A Matemática comporta um amplo campo de relações, regularidades e coerências que despertam a curiosidade e instigam a capacidade de generalizar, projetar, prever e abstrair, favorecendo a estruturação do pensamento e o desenvolvimento do raciocínio lógico." (BRASIL, 1997, p. 23). Nesse sentido, o estudo da Matemática é de suma importância para a estruturação do pensamento, assim como o desenvolvimento do pensamento lógico.

Para a realização deste trabalho teve a seguinte prerrogativa que norteou o rumo desta pesquisa, sendo: Como o ensino contextualizado por meio da utilização da criptografia pode auxiliar no processo de ensino-aprendizagem em temas relacionados à álgebra e análise combinatória?. Dispomos como objetivo geral: Investigar o ensino contextualizado por meio da utilização da criptografia, como ferramenta metodológica auxiliar no processo de ensino-aprendizagem em temas relacionados à álgebra e análise combinatória. Em relação aos objetivos específicos, temos: Relacionar o contexto da criptografia ao conhecimento algébrico e de análise combinatória ensinado no ensino médio, conforme BNCC; Destacar a contribuição da criptografia por meio da sua aplicação que resultou em grandes marcos históricos; Identificar a importância da contextualização do ensino da álgebra e

análise combinatória envolvendo criptografia, como cifra de César e sistema do código de barras. No decorrer deste trabalho será explicitado alguns tópicos de criptografia que podem ser abordados nas aulas de matemática, com isso contribuindo para o ensino contextualizado.

Os alunos da Educação Básica são dados a ênfase no estudo da Matemática, devido sua contribuição para criticidade do aluno. Segundo a Base Nacional Comum Curricular (BNCC) “O conhecimento matemático é necessário para todos os alunos da Educação Básica, seja por sua grande aplicação na sociedade contemporânea, seja pelas suas potencialidades na formação de cidadãos críticos, cientes de suas responsabilidades sociais.” (BRASIL, 1997, p. 23). Onde o professor fazendo a relação entre teoria e prática envolvendo o meio que o aluno se encontra, traz para si uma maior credibilidade perante sua aplicação de aulas contextualizadas, potencializando o processo de aprendizagem.

2 CRIPTOGRAFIA NA HISTÓRIA

A utilização da Criptografia surgiu com finalidades militares (SILVA, 2000), na necessidade de troca de informações, nas quais as forças inimigas não poderiam ter conhecimento. De modo sucinto, pode-se afirmar que o objetivo geral da Criptografia é enviar uma mensagem codificada a um receptor (ou destinatário) que só eles a compreendam, se por ventura, vir a ser interceptada por terceiros, estes não poderão entender, a menos que saibam a “chave” para decodificá-la.

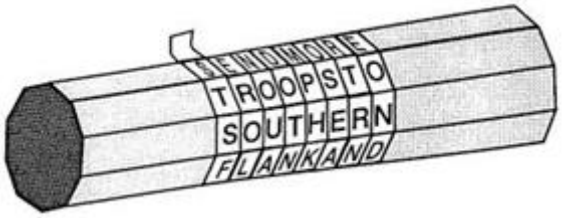
A importância da troca de informações parte desde muito cedo, derivando das diversas situações, na qual só o receptor e o destinatário têm acesso. Para Singh (2001, p. 21) “A comunicação secreta, quando é obtida por através de ocultação da mensagem, é conhecida como *estenografia,* nome derivado das palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever.” Com isso, vê-se que é relevante destacar o avanço dessa ciência que vem a progredir com o passar do tempo, buscando maior eficiência na troca de informações pelos seus usuários.

Com o decorrer do tempo houve a evolução da Criptografia, que a priori consistia em rearranjos de palavras ou anagramas, sendo este método muito limitado ou impossível de decodificar dependendo das palavras, por exemplo, a palavra LER, existem 6 possibilidades, pois cada letra não pode ser repetida, ou seja, para a primeira letra temos três possibilidades, para a segunda temos duas

possibilidades e para a terceira letra temos uma possibilidade, portanto teremos $3! = 3 \times 2 \times 1$, que resulta em 6 possibilidades, são elas: ELR, ELR, RLE, REL, LER, LRE. De modo análogo, ao analisar a palavra MATEMÁTICA teremos $10! = 3628800$ palavras, mas nessa quantidade de palavras teremos algumas repetidas, pois a letra A repete 3 vezes, as letras M e T se repetem 2 vezes cada, teremos $3! \times 2! \times 2!$ que são as permutações entre as letras que se repetem, ao dividirmos $10!$ por $3! \times 2! \times 2!$ obtemos 151200 possibilidades possíveis. Esse caso pode ser resolvido facilmente através de uma fórmula usada para o cálculo de casos em que ocorre a *permutação com repetição,* que seria $P_{3,2,2}^{10} = \frac{10!}{3!\times 2!\times 2!}$ resultando em $P_{3,2,2}^{10} = 151200$ palavras, ou seja, à medida que se tem mais letras, maior as possibilidades, implicando assim numa demanda de tempo proporcional a quantidades de letras que uma palavra possui.

O primeiro aparelho criptográfico militar é chamado *citale* (bastão de madeira) espartano (SINGH, 2001) que trata-se de um bastão de madeira que é enrolado com uma tira de couro, no qual é escrito a mensagem.

Figura 1 – *Citale* Espartano



Fonte: Singh (2001, p. 24).

A mensagem que é escrita na tira de couro num *citale* pelo emissor, em seguida é retirado o couro e colocado em outro *citale* de diâmetro diferente, fazendo com que as letras fiquem misturadas e as frases sem sentido, para o receptor descubra a mensagem basta colocar a tira de couro num *citale* de mesmo diâmetro.

Um meio usado pelo imperador de Roma, Júlio César, para enviar suas mensagens criptografadas utilizava o alfabeto, substituindo cada letra por outra que ficasse três casas à frente no alfabeto (vide tabela 1) desse modo constrói-se um alfabeto cifrado, sendo constituído pelas mesmas letras do alfabeto original (vide tabela 1). Para Suetônio (2002, p. 64) a cifra de César acontecia da seguinte maneira:

> Caso tivesse algum segredo a lhes transmitir, escrevia-lhes em linguagem cifrada, isto é, dispondo as letras em tal ordem que se não podia formar com elas nenhuma palavra. Para decifrá-las, era necessário trocar a quarta letra do alfabeto pela primeira, ou seja, o **d** no lugar do **a**, e assim consecutivamente.

Tabela 1 - Tabela do método de substituição utilizado por Júlio César

A.O	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.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	c

Fonte: Adaptado de Singh (2003, p.27)
Nota: A.O: Alfabeto Original, A.C: Alfabeto Cifrado

Utilizando a tabela 1, tomemos o seguinte exemplo de codificação de frase no alfabeto original: “EU GOSTO DE MATEMÁTICA”, a mesma palavra codificada no alfabeto de Cesar seria: “HXJRVWRGHPDWHPDWLFD”. Ao analisar a tabela, verifica-se que cada letra do alfabeto codificado fica três casas a frente em relação ao alfabeto original, ou seja, é múltiplo de 3. Para tanto pode-se realizar modificações para que sejam múltiplos de outros números, fazendo assim alfabetos distintos.

2.1 AS CONTRIBUIÇÕES DE ALAN TURING NA CRIPTOGRAFIA

O matemático e criptoanalista britânico Alan Turing (1912-1954) foi de fundamental importância para o desenvolvimento da criptografia, publicando trabalhos relacionados ao tema, como também na construção de sua máquina “de decifrar códigos” que viria a mudar o rumo da Segunda Guerra Mundial (1939 - 1945).

A máquina Enigma, sendo bastante famosa que foi utilizada pelos alemães durante a Segunda Guerra Mundial, possuindo vários de seus modelos. Os nazistas optaram pelo modelo conhecido como *Wehrmacht Enigma*. Estima-se que a quantidade usada durante a guerra era de 40 mil dessas máquinas (ROSSETO, 2018).

Figura 2 – Máquina Enigma

Fonte: SBC HORIZONTES

A Enigma sendo estimada em aproximadamente 12 kg, bem compacta para poder o manuseio em diferentes locais (SINGH, 2001) possui um teclado com 26 letras, com 3 rotores (misturadores) forneciam o total de $26 \times 26 \times 26$, ou seja, 17.576 ajustes diferentes e um quarto rotor denominado “refletor” estando estes alinhados, desse modo, a função do refletor nenhuma letra da mensagem seria decodificada nela mesma, assim que uma tecla é acionada os rotores movem uma posição, pois o refletor envia de volta através dos três rotores, por meio de uma rota diferente da que foi recebida (ROSSETO, 2018). Na II Guerra Mundial os nazistas utilizaram versões aprimoradas da Enigma para o aprimoramento da comunicação entre aliados “As versões militares alemãs da máquina de cifragem Enigma usavam fiação interna diferente, além de terem uma *Steckerbrett* (placa de conexões ou painel de plugues)” (MARRA, 2017, p. 151). Assim aumentando sua segurança na troca de informações entre aliados.

Para descobrir a quantidade de chaves possíveis da Enigma, iremos simplificar de modo que seja feito do ponto de vista mais didático, para isso considere uma versão da Enigma com apenas seis teclas com letras, podendo qualquer das 26 letras do alfabeto sem repetição e também levar em consideração algumas variáveis importantes que têm influência direta no cálculo das quantidades de chaves, são elas:

Orientação dos rotores. Sendo três rotores ajustados em 26 orientações distintas, temos: $(26)^3 = 26 \times 26 \times 26$, portanto 17.576 ajustes.

Disposição dos rotores. Existem três posições possíveis para o posicionamento dos rotores que é equivalente $3! = 3 \times 2 \times 1$, resultando em 6 ordens diferentes.

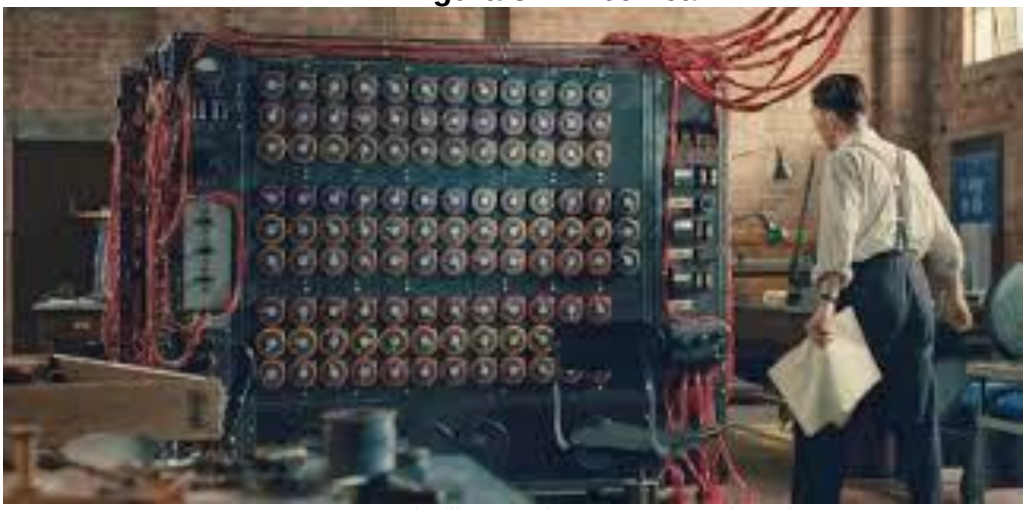
Painel de tomadas. O número que pode-se conectar, é trocar seis pares de letras dentre as 26 letras, é $100.391.791.500$.

O total de chaves possíveis resulta da multiplicação desses três números: $17.576 \times 6 \times 100.391.791.500 = 10.000.000.000.000.000$.

A máquina inventada por Turing teve como principal objetivo decodificar as mensagens enviadas pela Enigma. Para o funcionamento da máquina era utilizado uma cola que era disponível pela (biblioteca que se acumulava de mensagens codificadas), supondo que a cola seja a palavra **wetter** que se codifica em **ETJWPX** que do alemão significava clima, com a cola em mãos ele datilografava na máquina e se o texto cifrado não surgisse, era realizado ajustes , até que o texto correto surgisse, sendo essa a estratégia tentativa e erro, o problema que existiam $159.000.000.000.000.000.000$ de ajustes possíveis (SINGH).

Mesmo não tendo conhecimento dos ajustes utilizados na Enigma, podemos considerar o ajuste *S*. Com a primeira cifragem, é ajustado o primeiro rotor em uma casa na posição $S + 1$, a letra **e** é cifrada como **T**. Prosseguindo no processo de cifragem o rotor avança mais uma casa e cifra uma letra que não está no elo, desse modo ignoramos e o rotor avança novamente e chega a uma letra que está no elo. No ajuste $S + 3$, a letra **t** é cifrada como **W**.

Figura 3 – A *bomba*



Fonte: Cena do filme: Enigma - O Jogo da Imitação

As ideias de Turing resultaram em máquinas denominadas bombas que consistiam num conjunto de doze rotores Enigma conectados eletricamente, possibilitando lidar com elos maiores. “A unidade completa teria dois metros de altura, por dois de comprimento e um metro de largura” (SINGH, 2001, p. 197). Com o resultado positivo foi possível adiantar o término da II Guerra Mundial em

aproximadamente três anos.

2.2 CRIPTOGRAFIA NO CÓDIGO DE BARRAS

Com o decorrer do tempo a criptografia se tornou bastante comum no cotidiano das pessoas, que uma das formas mais comum que se encontra é por meio do código de barras, que está presente em diversos produtos quando adquirimos, como: eletrodomésticos, eletroeletrônicos e livros.

No meio escolar está presente nos livros que os discentes utilizam para estudar, e também visto como entretenimento entre grupos de alunos que usam a criptografia para enviar mensagens. Em cada livro existe um código ISBN (*International Standard Book Number*) que serve para identificar obras, como livros, revistas e que consiste em algarismos agrupados em quatro partes, sendo este separados por hífen ou espaço em branco, as partes formadas por algarismos tem como objetivo identificar o país, editora, número que a editora concede a obra e a última parte que é um único dígito, chamado de dígito verificador (ISBN, 2011).

No sistema de código de barras utiliza-se 13 dígitos, sendo que os primeiros 12 dígitos multiplica-se de modo alternado por 1 e 3 (TAKAHASHI, 2015). Para a obtenção do dígito de verificação (denotaremos de *X*), sendo a soma dos produtos ponderados dos primeiros 12 dígitos, com isso subtrai-se por 10 e tem-se o dígito de verificação, vale ressaltar que caso o cálculo do dígito de controle resulte em 10, o dígito de controle será 0. De modo simplificado seja os 12 primeiros dígitos do código de barras: $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}$, com $a \in$ IN. Para calcularmos o dígito verificador, utilizamos a seguinte fórmula:

$Y = \sum_{i=ímpar;j=par}^{12} 1.(a_i) + 3.(a_j)$.

Com o resultado do somatório (denotaremos de *Y*), encontra-se o primeiro número múltiplo de dez após (denotaremos de *Z*), com isso o dígito verificador será o resultado da subtração *Z* por *Y*, ou seja, $X = Z - Y$.

Usando o seguinte processo para calcular o dígito de verificação para o ISBN 978-85-510-0249-X

Aplicando $Y = \sum_{i=ímpar;j=par}^{12} 1.(a_i) + 3.(a_j)$, temos:

$$Y = 1.a_1 + 3.a_2 + 1.a_3 + 3.a_4 + 1.a_5 + 3.a_6 + 1.a_7 + 3.a_8 + 1.a_9 + 3.a_{10} + 1.a_{11} + 3.a_{12}$$

$$Y = 1.9 + 3.7 + 1.8 + 3.8 + 1.5 + 3.0 + 1.1 + 3.0 + 1.5 + 3.5 + 1.9 + 3.8$$

$$Y = 1.(9+8+5+1+5+9) + 3.(7+8+0+0+5+8)$$

$$Y = 1.37 + 3.28 \Rightarrow Y = 121.$$

Com o resultado do somatório $Y = 121$, obtemos $Z = 130.$ Logo, o dígito verificador $X = Z - Y \Rightarrow X = 130 - 121 \Leftrightarrow X = 9.$ Vale ressaltar que os cálculos efetuados acima são análogos a outros códigos de barras de 13 dígitos.

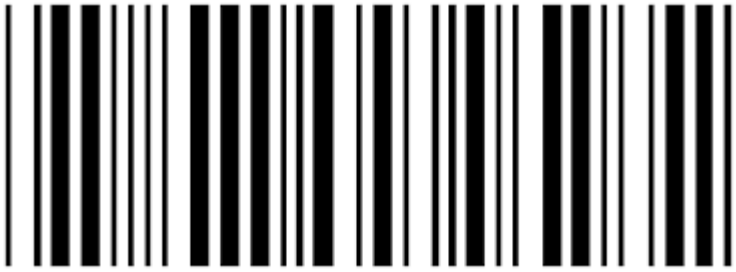
No Exame Nacional do Ensino Médio (ENEM) na sua edição de 2002 na parte de matemática foi abordada na questão 27 sobre o código de barras numa perspectiva de análise combinatória. Seja $a_1, a_2, a_3, a_4, a_5,$ com $a_n \in$ IN e $n \subset [1,5]$, onde a_n é referente aos dígitos do código de barras que a questão refere-se (ENEM, 2002), para isso teremos duas situações:

Na 1º situação, fixamos o $a_3 = 1,$ com isso a_1 e a_2 tem duas possibilidades sendo elas 0 ou 1, para os dígitos a_4 e a_5 é de apenas uma possibilidade cada, pois devem ser iguais aos dígitos a_1 e a_2, resultando $2 \times 2 \times 1 \times 1 \times 1 = 4$ possibilidades.

Na 2º situação, fixaremos o $a_3 = 0,$ teremos o caso análogo ao anterior, resultando assim $2 \times 2 \times 1 \times 1 \times 1 = 4$ possibilidades. Somando a 1 (primeira) e 2 (segunda) situação, teremos o total de 8 possibilidades, desconsiderando as possibilidades de todos os dígitos serem iguais a 0 e iguais a 1, resulta em $8 - 1 - 1 = 6$ possibilidades.

O código de barras sobre uma perspectiva em análise combinatória podemos ter como exemplo da questão 4 abordada na prova *Canguru de Matemática Brasil 2020*, na prova Nível P, que era mencionado sobre um código de barras constituído de 17 barras, com as cores preta e branca, sendo a primeira e a última de cor preta. As barras pretas podendo ser largas e estreitas. Para esse código de barras existem três barras brancas a mais que as barras pretas largas. Nesse sentido, é questionado sobre a quantidade de barras pretas estreitas.

Figura 4 – Código de barras



Fonte: Manual de Usuário do Leitor BR-400

Pelo enunciado, sabemos que o total de barras desse código é 17, sendo

brancas e pretas, com a primeira e a última barra de cor preta. Portanto, o código possui uma barra preta a mais em relação às brancas, com isso temos a soma de dois números naturais que resultam em 17, são eles 9 e 8, representando respectivamente barras pretas e brancas no código.

Nessa questão sabemos que existem 3 barras brancas a mais que as barras pretas largas, com isso temos $8 - 3 = 5$ barras pretas largas. Logo, o total de barras pretas é 9, assim descobrimos a quantidade de barras pretas estreitas que é $9 - 5 = 4$.

Com isso, temos duas alternativas de se abordar o código de barras, sendo este presente no cotidiano do estudante, existindo outras maneiras de contribuir para o estudo da matemática, ocorrendo de variações que estão convergentes com a realidade do aluno e com a contribuição com a criatividade do docente que ministra a disciplina, fazendo maneiras melhores de aplicar em sala de aula.

3 SUGESTÃO DE APLICAÇÃO

Para a aplicação em sala de aula é importante ministrar uma aula de matemática sobre os assuntos: expressões algébricas e análise combinatória, é sugerido o domínio desses conteúdos por parte do professor, para relacionar tais conteúdos aos conceitos matemáticos utilizados na criptografia na resolução das atividades.

Podendo a aula acontecer de forma expositiva e posteriormente sugerida atividade impressa de cunho avaliativo sobre o assunto ministrado, de tal forma que possibilite uma contextualização do ensino, facilitando no processo de ensino aprendizagem.

Nesse sentido, o trabalho em grupo pode ser uma alternativa para que os discentes desenvolvam a comunicação e respeito entre os colegas por meio de trabalho em grupos. Para isso a sala pode ser dividida em grupos 1, 2, 3... respectivamente definidos como: $G_1, G_2, G_3,$ ... sendo disponibilizado o uso do *smartphone* na resolução das atividades, posteriormente a discussão da resolução da atividade proposta.

Tendo em vista a preparação do docente e o pleno domínio de conteúdo que compete como conhecimento prévio na aplicação do ensino da matemática por meio da criptografia. É importante ressaltar sobre o surgimento da criptografia, como

também dos sujeitos que faziam uso e sua finalidade, com isso ressaltar sua importância para o desenvolvimento da história da humanidade.

Uma maneira de verificar a assimilação dos conteúdos propostos, sugere-se a realização de um teste diagnóstico, sendo uma lista de questões contextualizadas a respeito da criptografia contendo cifra de César com alfabeto de múltiplo três, decifrar mensagens com expressões numéricas e do código de barras. Com isto, é possível verificar o nível em que se encontra o discente em relação a matemática básica.

4 METODOLOGIA

Diante do momento singular em que foi produzido o presente trabalho, o mundo passa por uma pandemia de alta calamidade, que por ventura a assegurar pela segurança e saúde dos pesquisadores e das demais pessoas que possivelmente iriam participar, decidiu-se que a modalidade que abrangesse tais requisitos é a pesquisa bibliográfica para a produção deste trabalho.

Para isso a pesquisa bibliográfica ocorreu em anais de congresso, artigos, dissertações e principalmente na revista Sociedade Brasileira de Ensino de Matemática (SBEM), sendo que os trabalhos tinham como prerrogativa “A utilização da Criptografia como ferramenta metodológica no ensino da matemática”.

Com a realização da pesquisa bibliográfica foi analisado 8 (oito) artigos, dentre os artigos temos 2 (duas) dissertações de mestrado, 7 (sete) livros e 3 (três) documentos, tal pesquisa norteou o rumo da pesquisa. A pesquisa bibliográfica tal como definido por Lakatos e Marconi (1991, p. 183):

> A pesquisa bibliográfica, ou de fontes secundárias, abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico, etc. [...] Dessa forma, a pesquisa bibliográfica não é mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras.

Para tanto, optou-se por realizar um trabalho em tal modalidade de pesquisa, buscando relacionar tópicos de matemática que estão presentes na criptografia com matemática estudada na educação básica como meio de contextualizar o ensino, facilitando o processo de ensino aprendizagem. Tais assuntos a serem abordados de forma contextualizada podem prover alcançar habilidades e competências previstas na BNCC.

O objetivo principal desta pesquisa é investigar as contribuições da Criptografia no ensino da matemática como meio de auxiliar no processo de ensino-aprendizagem para alunos, que de preferência estejam cursando o 2º ano do ensino médio, pois nesse período é realizado um estudo especificamente em conteúdos de cálculo algébrico e análise combinatória.

A respeito do ensino da álgebra os Parâmetros Nacionais Curriculares (PCNs) destacam que “O estudo da Álgebra constitui um espaço bastante significativo para que o aluno desenvolva e exercite sua capacidade de abstração e generalização além de lhe possibilitar a aquisição de uma poderosa ferramenta para resolver problemas”.(BRASIL, 1998, p. 115). Dessa forma notamos a importância do estudo da álgebra no desenvolvimento do pensamento matemático para os alunos na Educação Básica.

Como também aprimorasse o desenvolvimento do raciocínio lógico matemático, vale ressaltar que “[...] é preciso desenvolver no aluno a habilidade de elaborar um raciocínio lógico e fazer uso inteligente e eficaz dos recursos disponíveis, para que ele possa propor boas soluções às questões que surgem em seu dia-a-dia, na escola ou fora dela.” (DANTE, 2007, p. 11). Com isso, vê-se um ponto de vista importante a se abordar nas aulas de matemática no que diz respeito sobre o ensino contextualizado como forma de metodologia que possa ser utilizada nas aulas para propor o dia a dia do discente nas aulas.

Nesse sentido, é perceptível a importância do raciocínio lógico tanto na vida do estudante, sendo-a capaz de instigar a tomar melhores decisões. Para tanto, optou-se pela realização de uma abordagem no trabalho que demonstrasse algumas aplicações de criptografia que envolve determinados assuntos que são abordados na educação básica.

5 RESULTADOS E DISCUSSÕES

Com a obtenção de informações que a pesquisa bibliográfica, foi possível associar tópicos de criptografia no processo de ensino-aprendizagem em matemática. É importante ressaltar a convergência desses tópicos de matemática com o preparo do docente e com a realidade que o estudante está inserido.

Para a melhoria do processo de ensino-aprendizagem em matemática pode-se aplicar metodologias de ensino que facilite o aprendizado do discente na educação básica, pois é importante desenvolver no aluno a habilidade de

desenvolver um raciocínio lógico e de fazer uso inteligente, para que ele possa propor soluções a problemas que surgem em sua realidade (DANTE, 2007).

Diante disso, uma alternativa é a utilização de aulas contextualizadas com a realidade do aluno, que esteja presente em diversos aspectos da vida, tornando mais viável a contextualização fazendo referências a esses aspectos, sendo a criptografia em código de barras, o uso de senhas, como também as mensagens codificadas, como meio de entretenimento, sendo uma alternativa que abrange tais requisitos é o ensino da matemática por meio da criptografia. É importante frisar que criptografia surgiu com finalidades militares (SILVA, 2000) e que, com o decorrer do tempo ela se desenvolveu a fim de suprir as necessidades que surgiam para a proteção de troca de informações, tais aspectos em seu desenvolvimento está presente em diversos campos da vida do aluno, por meio da matemática que é utilizada na criptografia.

Um bom conhecimento matemático é importante para o aluno da educação básica, facilitando na formação de cidadãos críticos, como relata a BNCC “O conhecimento matemático é necessário para todos os alunos da Educação Básica, seja por sua grande aplicação na sociedade contemporânea, seja pelas suas potencialidades na formação de cidadãos críticos.” (BRASIL, 1997, p. 23). Para que isso ocorra é de suma importância o preparo do professor, sendo este responsável por conduzir a aula.

Como é mencionado pela BNCC sobre importância que a matemática tem na formação de cidadãos críticos, uma alternativa a se fazer é por meio da criptografia. Para Oliveira e Kripka (2011, p. 12) “Acredita-se que a inclusão de atividades que envolvam conceitos de criptografia pode ajudar a diminuir a existência de aulas mecânicas, através de atividades práticas [...]” Com a inserção de atividades presentes na vida do discente, sendo a criptografia uma delas, pode-se contribuir nas aulas de matemática.

Nesse sentido, o professor deve estar apto a demonstrar a matemática implícita na criptografia que é utilizada na vida do aluno, relacionando ao contexto da sala de aula, para que possa facilitar na assimilação de conteúdos que são abordados na sala de aula, tornando uma aula diferente do convencional, do tipo expositiva e tratando-a de um modo diferente que esteja relacionada ao cotidiano do aluno.

6 CONSIDERAÇÕES FINAIS

A partir deste estudo, foi possível perceber que o estudo da matemática pode ser diversificado, de modo que convirja com a realidade que o aluno está inserido, podendo assim expor a importância do estudo da matemática para o desenvolvimento da humanidade, isso pode ser feito através do estudo da criptografia, sendo este presente em diferentes contextos da vida humana, desde a compra no supermercado, até abordagem de conteúdos matemáticos que são usados na criptografia.

Dessa forma, acredita-se que a utilização da criptografia no ensino da matemática para o ensino básico é uma alternativa a se considerar pelo professor, para que possa explorar tópicos matemáticos de forma contextualizada e diversificada com a realidade presente do aluno.

Diante disso, espera-se que este trabalho contribua e motive os professores de matemática a utilizarem o estudo da criptografia em suas aulas de matemática, podendo assim contribuir no desenvolvimento de habilidades e competências em que o aluno necessita no decorrer de estudos posteriores.

REFERÊNCIAS

BEMATECH. **Manual de Usuário do Leitor BR-400.** Disponível em: <https://www.bematech.com.br/wp-content/uploads/2019/12/MAN-USR-BR-400-R1.0.pdf> . Acesso em: 28 out. 2020.

BRASIL. **Base Nacional Comum Curricular (BNCC).** Educação é a Base. Brasília, MEC/CONSED/UNDIME, 2017.

BRASIL. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais: Matemática**. Brasília. 1998. 148. Disponível em : <http://portal.mec.gov.br/seb/arquivos/pdf/matematica.pdf>. Acesso em: 13 abr. 2020.

BRASIL. **Parâmetros Curriculares Nacionais: Matemática** / Secretaria de Educação Fundamental. – Brasília : MEC/SEF, 1997. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/livro03.pdf>. Acesso em: 28 fev. 2020.

CHEVALLARD, Y. (1991) **La Transposition Didactique**: Du Savoir Savant au Savoir Ensigné. Grenoble, La pensée Sauvage.

CYPHER RESEARCH LABORATORIES. **A Brief History of Cryptography.** Disponível em: <http://www.cypher.com.au/crypto_history.htm> . Acesso: 09 out. 2020.

DANTE, Luiz Roberto. **Didática da Resolução de Problemas de Matemática**. 12. ed. São Paulo: Editora Ática. 2007.

DELIZOICOV, D. **Problemas e Problematizações.** In: PIETROCOLA, Maurício (org.). Ensino de Física: conteúdo, metodologia e epistemologia numa concepção integradora. Florianópolis: Ed. da UFSC, 2001. 236p.

ENEM 2002. **Exame Nacional do Ensino Médio**. Ministério da Educação Instituto Nacional de Estudos e Pesquisas Educacionais PROVA 1 - AMARELA. Disponível em: <http://download.inep.gov.br/educacao_basica/enem/provas/2002/2002_amarela.pdf >. Acesso em: 30 out. 2020.

HAZZAN. Samuel, **Fundamentos de Matemática Elementar - vol 5**. 3. ed. Editora Atual, 19.

LAKATOS, Eva M.; MARCONI, Marina de A. **Fundamentos de Metodologia Científica**. 3. ed. rev. e ampl. São Paulo: Atlas, 1991.

MARRA, George Mendes. **O JOGO DA MÍMESE E O USO DA CRIPTOGRAFIA**. Pontifícia Universidade Católica de Goiás Pró-reitoria de pós-graduação e pesquisa escola de formação de professores e humanidades. Goiânia 2017.

Manual do usuário ISBN. **The International Standard Book Number System.** Disponível em: <https://www.isbn-international.org/sites/default/files/Manual%20usu%C3%A1rios%20ISBN%20-%206%20edi%C3%A7%C3%A3o%20%28Portuguese%29.pdf>. Acesso em: 12 fev. 2020.

MICOTTI, M. C. O. **O ensino e as propostas pedagógicas**. In: BICUDO, M. A. V. Pesquisa em educação matemática: concepções e perspectivas. São Paulo: Editora UNESP, 1999.

OLIVEIRA, D.; KRIPKA, R. M. L. **O Uso da Criptografia no Ensino de Matemática**. 2011. Disponível em: < https://docplayer.com.br/5004244-O-uso-da-criptografia-no-ensino-de-matematica.html >. Acesso em: 24 fev. 2019.

ROSSETO, Cintia Kohori. **Criptografia como Recurso Didático: Uma Proposta Metodológica aos Professores de Matemática**. UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO” Campus de Presidente Prudente Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT). Presidente Prudente 2018.

SBC HORIZONTES. **Alan Turing e a Enigma**. Disponível em: < http://horizontes.sbc.org.br/index.php/2016/11/alan-turing-e-a-enigma/ > . Acesso em: 01 nov. 2020.

SILVA, A. A. **Números, Relações e Criptografia.** Departamento de Matemática - UFPB, Paraíba, 2000.

SINGH, Simon. **O livro dos códigos** / Simon Singh; tradução de Jorge Calife. - Rio de Janeiro: Record, 2001.

SUETÔNIO. **A Vida dos Doze Césares**. trad. Sady-Garibaldi. 2 ed. São Paulo. Ediouro. 2002.

TAKAHASHI, Cássia Regina dos Santos. **Ensinando matemática através dos códigos de barras**. Ciência e Natura, Santa maria, v. 37 Ed. Especial PROFMAT, 2015, p. 278-288. Disponível em: https://sca.profmat-<sbm.org.br/sca_v2/get_tcc3.php?id=37577>. Acesso em: 12 abr. 2020.

TAMAROZZI, Antônio Carlos. **Codificando e decifrando mensagens**. In Revista do Professor de Matemática 45*,* São Paulo: Sociedade Brasileira de Matemática, 2001. Disponível em: <http://www.educadores.diaadia.pr.gov.br/arquivos/File/2010/veiculos_de_comunicacao/RPM/RPM45/RPM45_08.PDF>. Acesso em: 24 fev. 2019.