CRIPTOGRAFIA: UMA FERRAMENTA DE ENSINO DAS OPERAÇÕES MATRICIAIS

Naiara Pereira Tavares[1]; Francisca Edna Ferreira Felix[1]; Maria Cassiana Pereira Gonçalves[2]; Reginaldo Amaral Cordeiro Junior[3].

[1]*Instituto Federal de Educação Ciência e Tecnologia da Paraíba-Campus Cajazeiras, naiara.pereira@academico.ifpb.edu.br*

[1]*Instituto Federal de Educação Ciência e Tecnologia da Paraíba-Campus Cajazeiras, edna.felix@academico.ifpb.edu.br*

[2]*Instituto Federal de Educação Ciência e Tecnologia da Paraíba-Campus Cajazeiras, maria.cassiana@academico.ifpb.edu.br*

[3]*Instituto Federal de Educação Ciência e Tecnologia da Paraíba-Campus Cajazeiras, reginaldo.cordeiro@ifpb.edu.br* .

Resumo: Desde a antiguidade houve a necessidade de se comunicar de maneira sigilosa, nas guerras, por exemplo, os grandes generais tinha a preocupação de se comunicar secretamente entre as bases e assim desenvolver seus planos de ataques em segurança. Os primeiros relatos sobre a utilização da criptografia aconteceram nas civilizações antigas quando os Egípcios usaram os hieróglifos para manter documentos importantes em segurança, e desde então, muitos estudiosos se propuseram a estudar sobre essa técnica, alcançando grandes avanços e tornando-a uma importante aplicação da Matemática. Nesse sentido, o presente trabalho tem por objetivo utilizar a criptografia como uma ferramenta de ensino de conteúdos matemáticos, tendo a sua relevância em trazer ao debate a importância de ensinar a Matemática de forma mais articulada com a realidade dos discentes, mostrando uma forma de se trabalhar essa disciplina a partir de uma de suas aplicações importantes para a sociedade atual. Para isso, realizamos um estudo bibliográfico sobre a criptografia, abordando a sua evolução histórica e os conceitos matemáticos aplicados a essa técnica, destacando a Cifra de Hill a qual é uma técnica criptográfica baseada na Álgebra Linear, mais especificamente nas operações matriciais e na aritmética modular. E como parte final deste trabalho, elaboramos uma sequência didática para auxiliar os professores da Educação Básica no ensino das operações matriciais utilizando a criptografia como uma alternativa metodológica em sala de aula, visando a melhoria do processo de ensino aprendizagem.

Palavras-chave: Criptografia, Matemática, Matrizes, Sequência Didática.

1 Introdução

A criptografia é uma técnica utilizada para a troca de informações de maneira segura, ou seja, é uma forma de comunicação secreta em que somente o emissor e o receptor conseguem ter acesso as informações trocadas.

Essa técnica é utilizada desde os primórdios para a troca de informações sigilosas principalmente nas guerras. Para Singh (2001) “A história dos códigos e de suas chaves é a história de uma batalha secular entre os criadores de código e os decifradores, uma corrida armamentista intelectual que teve um forte impacto na história humana”. Assim, os grandes estudiosos estavam sempre em busca de “quebrar” a técnica criptográfica criada afim de desenvolver outra mais segura.

Hoje, a criptografia é bastante utilizada como um meio de segurança em operações no nosso cotidiano facilitando o acesso a sistemas de caixas eletrônicos, páginas da internet e outros meios que necessitam manter a segurança na transmissão de dados. Podemos destacar que a criptografia é uma aplicação da matemática, visto que as técnicas criptográficas mais seguras são fundamentadas em algumas áreas da Matemática, tais como Álgebra Linear, Matemática Discreta e Teoria dos Números. Daí, surge então a ideia que norteia o nosso estudo, trabalhar a criptografia como uma aplicação de conteúdos matemáticos.

Segundo Tamarozzi(2001) citado por Clarrissa de Assis Olgin et al. (2011), "o tema Criptografia possibilita o desenvolvimento de atividades didáticas envolvendo os conteúdos de matrizes e funções que se constituem em material útil para exercícios, atividades e jogos de codificação, onde o professor pode utilizá-los para fixação de conteúdos."

Nesse sentido, a utilização de uma sequência didática, pode auxiliar o professor a trabalhar interligando conteúdos matemáticos a situações do cotidiano, influenciando de forma direta o desenvolvimento de habilidades e competências na resolução de problemas. Possibilitando ao aluno a autonomia no processo de aprendizagem, tornando-o mais autoconfiante e concentrado na realização das atividades.

Neste trabalho temos por objetivo tratar a criptografia como uma ferramenta de ensino, para tanto discutiremos primeiramente sobre a criptografia abordando um breve histórico e alguns conceitos existentes no meio criptográfico. Posteriormente analisaremos a fundamentação matemática evidenciando o estudo de matrizes e congruência, uma vez que tais assuntos são subsídio para a cifra de Hill a qual será evidenciada através de uma sequência didática que poderá nortear professores de Matemática no estudo de matrizes.

Portanto, a relevância dessa trabalho consiste não só no fato de estudar a criptografia e a sua aplicação como introdução de conteúdos matemáticos. Mas sobretudo, em trazer ao debate a importância de trabalhar a matemática de forma mais articulada com a realidade. Desse modo, há a possibilidade de motivar o aluno à aprendizagem, mostrando a importância de aprender matemática.

A metodologia utilizada neste trabalho quanto aos objetivos e aos procedimentos técnicos tem caráter exploratório, a qual envolve um levantamento bibliográfico a cerca da criptografia e dos seus aspectos históricos como também dos conceitos matemáticos que embasam teoricamente o meio criptográfico. Assim, o presente artigo tem caráter qualitativo, pois não se apoia em dados estatísticos, mas contribui significativamente para o desenvolvimento do pensamento cientifico, conforme afirma Trivino:

> [...] Sem dúvida alguma, muitas pesquisas de natureza qualitativa não precisam apoiar-se na informação estatística. Isto não significa que sejam especulativas. Elas têm um tipo de objetividade e de validade conceitual, que contribuem decisivamente para o desenvolvimento do pensamento científico [...] (TRIVINOS, 1987, p.118)

Posteriormente ao estudo bibliográfico a equipe de autores desenvolveu uma sequência didática para o ensino de matrizes no Ensino Médio relacionando-o com aplicação na criptografia.

2 Criptografia

A criptografia foi desenvolvida a partir da necessidade de manter a troca de mensagens sigilosas em segurança e é utilizada desde a antiguidade, desempenhando um papel fundamental durante os períodos de guerra. A origem da palavra vem do grego kryptós que significa escondido e gráphein que significa escrita, dessa forma, criptografia significa escrita escondida. Essa técnica que vem se aprimorando ao longo dos anos, alcançando avanços exponenciais, tem fundamentação baseada na Matemática.

2.1 Breve Histórico

Os primeiros relatos a cerca da utilização da criptografia, aconteceram em aproximadamente 1900 a.C quando os egípcios utilizaram os hieróglifos para codificar documentos importantes. No século V a.C, o exercito espartano também utilizava a criptografia para trocar as suas mensagens de maneira mais segura. Essa cifra que ficou conhecida como cítalas, utilizava cilindros com o mesmo diâmetro para trocar mensagens, como descreve Jesus(2013):

> Para codificar uma mensagem, o emissor inicialmente enrolava uma faixa de pergaminho ao redor da cítala, de modo que espirasse o cilindro. Depois, escrevia a mensagem sobre o pergaminho, ao longo do comprimento da cítala. Desenrolando-se o pergaminho a mensagem fica codificada. Para decifrar a mensagem era necessário, que o receptor tivesse, uma cítala de mesmo diâmetro para enrolar a tira de como ler a mensagem.

Um outro método conhecido é Cifra de Políbio ou quadrado de Políbio que foi desenvolvido pelo grego Políbio por volta de 200 a.C. a 118 a. C. É uma cifra de substituição que consiste numa tabela quadrada (mesmo número de linhas e colunas), onde os caracteres são disponibilizados um em cada célula desta tabela.

Os romanos também desenvolveram uma cifra bastante conhecida, a Cifra de César, que recebe esse nome em homenagem a Júlio César que usou para se comunicar com seus generais. É um tipo de cifra de substituição na qual cada letra o alfabeto é substituída por outra, por exemplo, numa troca de três posições, A seria substituído por D, B por E e assim sucessivamente.

Os franceses também tiveram seu papel importante no desenvolvimento da Criptografia com a Cifra de Vigenère, a qual foi desenvolvida pelo francês Blaise de Vigenère no século XVI. É uma cifra de substituição polialfabética que consiste na utilização de mais de um alfabeto cifrante. Por alguns séculos foi considerada como a "cifra indecifrável", até que em 1850 o matemático inglês Charles Babbage "quebrou" esta cifra.

Destacamos mais uma cifra criada em 1929 pelo norte americano Lester S. Hill, a qual é chamada de Cifra de Hill. Baseada na Álgebra Linear, mais especificamente, em transformações matriciais e na aritmética modular.

Um método de criptografar mensagem que ficou conhecido na história foi a Máquina Enigma, utilizada na 2ª Guerra Mundial pelos alemães. Patenteada por Arthur Scherbus em 1918, começou a ser utilizada na Europa por volta de 1920, a codificação dessa máquina era de difícil decifração, pois era necessário ter outra máquina para poder fazer o processo de decodificação. A Máquina Enigma tinha uma característica que revolucionava o meio criptográfico pois era um dispositivo eletro-mecânico composto por um teclado, um painel com letras que acendiam, um plugbord, um refletor e um mecanismo de rotores.

Essa técnica alemã parecia infalível, até que o matemático Alan Turing e sua equipe desenvolveram uma máquina capaz de decifrar o "Enigma" dos nazistas e assim conseguiram derrotar mais depressa a força da Alemanha. A máquina desenvolvida por Turing e seus companheiros se tornou um protótipo dos computadores modernos.

Até meados dos anos 70 a chave utilizada na criptografia era a chave privada, mas em 1976 devido aos avanços tecnológicos os pesquisadores Whitfield Diffie e Martin Hellman desenvolveram a criptografia de chave púbica. Através desse método um emissor e receptor podem combinar uma chave por meio de um canal inseguro sem que um espião possa interceptar e descobrir a chave de decodificação, esse método é baseado nas operações com logaritmos discretos.

Em 1978 foi desenvolvida a criptografia RSA, o nome que esse método recebe é em homenagem aos seus criadores Ronald Rivest, Adi Shamir e Leonard Adleman, os quais eram professores do Instituto de Tecnologia de Massachusetts (MIT).

Baseada principalmente na teoria dos números, a criptografia RSA é considerada um dos métodos mais seguros para criptografar mensagens, por ser uma criptografia de chave assimétrica que tem como base um algoritmo que requer duas chaves, uma pública e outra privada.

Veremos a seguir que na criptografia existem alguns termos definidos conforme o seu modo de utilização, como por exemplo, cifra e chave. As quais podem ser classificadas em cifra de substituição e tranposição e as chaves como simétrica ou assimétrica.

2.2 Cifra de substituição e de transposição

Os métodos de cifrar são divididos em dois tipos: método de cifragem por substituição e método de cifragem por transposição.

No primeiro método a mensagem é codificada de modo que cada um dos seus caracteres é substituído por um outro de acordo com uma tabela de substituição. As cifras de substituição podem ser ainda classificadas como cifra de substituição monoalfabética, onde as letras do texto cifrado podem ser substituídas por letras ou símbolos. Outra classificação dada é a cifra de

substituição polialfabética, em que uma mesma letra do texto claro pode ser substituída por diferentes símbolos ou letras no texto cifrado.

O segundo método de cifragem permite que as letras permutem, ou seja, há apenas uma troca de posição entre as letras do texto não codificado e o cifrado, as letras permanecem com a sua identidade.

2.3 Criptografia de Chave Simétrica e de Chave Assimétrica

A criptografia de chave simétrica é um tipo de criptografia que utiliza somente uma chave tanto para codificar como para decodificar uma mensagem. Na criptografia simétrica os algoritmos usados são mais simples que na criptografia assimétrica, o que leva o processo a ser mais rápido, possibilitando a cifragem e a decifragem de uma grande quantidade de dados em um espaço de tempo curto.

Na criptografia de chave assimétrica utiliza-se duas chaves, a chave pública e a chave privada, em conjunto são conhecidas como par de chaves. Os algoritmos utilizados são mais complexos, o que torna o processo de criptografar e descriptografar muito mais lento do que na simétrica.

A criptografia de chave assimétrica é considerada mais segura que a criptografia de chave simétrica, devido ao uso das duas chaves, onde a chave para criptografar é diferente da chave utilizada para descriptografar.

3 Fundamentação Matemática

A criptografia utiliza muitos conteúdos matemáticos para garantir uma maior segurança, mas evidenciaremos apenas o estudo de matrizes, abordando a definição de matrizes, mostrando alguns tipos especiais, as operações matriciais e a matriz inversa. Para em seguida, abordarmos congruência e inverso modular, pois tais assuntos dão subsídio para a técnica criptográfica que evidenciaremos neste trabalho.

3.1 Matrizes

As definições apresentadas aqui podem ser encontradas no livro de Gelson Iezzi e Samuel Hazzan, Fundamentos da Matemática Elementar V.04.

Definição 3.1. Chama-se de matriz uma tabela formada por m linhas e n colunas, sendo denominada de matriz m por n e indica-se $m \times n$. Os elementos de uma matriz qualquer M, são

representados por a_{ij}, onde i indica a linha e j a coluna.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

3.1.1 Alguns tipos de Matrizes

- **Matriz quadrada** é aquela que possui o mesmo número de linha e coluna, ou seja $m = n$
- **Matriz nula** é todo matriz que $a_{ij} = 0$ para todo ij
- **Matriz coluna** é toda matriz que $n = 1$
- **Matriz linha** é toda matriz que $m = 1$
- **Matriz identidade** é toda matriz quadrada que $a_{ij} = 1$, para $i = j$ e $a_{ij} = 0$, para $i \neq j$
- **Matriz diagonal** é todo matriz quadrada eu $a_{ij} = 0$, para $i \neq l$

3.1.2 Operações com Matrizes

- **Adição**
  Dadas duas matrizes $A = (a_{ij})$ e $B = (b_{ij})$ de mesma ordem, obtemos $C = (c_{ij})$, para $c_{ij} = a_{ij} + b_{ij}$. Ou seja, $C = A + B$, onde cada elemento de C é resultado da soma dos correspondentes de A e B.
- **Produto de um número por matriz**
  Dado uma constante C e uma matriz $A = (a_{ij})$, obtemos o produto CA como uma matriz $B = (b_{ij})$, como $b_{ij} = C \cdot a_{ij}$. Ou seja, a matriz B é constituída pelo produto de C por cada um dos elementos de A.
- **Produto de matrizes**
  Dadas as matrizes $A = (a_{ij})$ e $B = (b_{rs})$. Definimos o produto de A por B como $AB = (c_{uv})$, onde $c_{uv} = \sum_{k=1}^{n} a_{uk} b_{kv} = a_{u1} b_{1v} + \cdots + a_{un} b_{nv}$.
- **Matriz transposta**
  Dada a matriz $A = (a_{ij})$, chamamos de transposta de A a matriz $A^t = (a_{ji})$. Ou seja, as linhas da matriz A são iguais as colunas da matriz B.
- **Matriz Inversa**
  Dada uma matriz A de ordem n. A é inversível se, e somente se, existe uma matriz B de ordem n, tal que

$$AB = BA = I_n$$

3.2 Congruência

Definição 3.2. Se a e b são inteiros dizemos que a é congruente a b módulo m se $m \mid (a-b)$ e denotamos por $a \equiv b (\mathrm{mod}\, m)$. Ou seja, a é congruente a b módulo m se $(a-b)$ é um múltiplo de m.

3.2.1 Inverso Modular

Para cada a não-nulo, o seu inverso multiplicativo na Aritmética Modular usual é:

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Isso é correspondente ao seguinte conceito

Definição 3.3. Dado um número a em $\mathbb{Z}_m$, dizemos que a^{-1} em $\mathbb{Z}_m$ é o inverso multiplicativo de a módulo m se $aa^{-1} = a^{-1}a \equiv 1 \,(\mathrm{mod}\, m)$.

Em matrizes, dizemos que uma matriz A em Z_m é invertível módulo m se existe uma matriz B tal que

$$AB = BA \equiv I \,(\mathrm{mod}\, m)$$

4 Criptografia através de Matrizes

Nesta seção abordaremos duas técnicas criptográfica que se fundamentam no estudo das operações matriciais e que podem auxiliar os professores de Matemática no processo de ensino aprendizagem.

A primeira utiliza uma técnica simples já abordada em alguns livros didáticos, como pode ser encontrado no livro Quadrante - Matemática 2 de Chavante e Prestes (2016), o qual apresenta o assunto de criptografia como aplicação prática cotidiana para o conteúdo de matriz. O método de codificação e decodificação que o livro aborda é feito da seguinte forma:

- Considera-se a tabela a seguir, em que cada letra do alfabeto é representada por um número.

Tabela 4.1: Alfabeto com o seu respectivos valores numéricos

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
1	2	3	4	5	6	7	8	9
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
10	11	12	13	14	15	16	17	18
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**espaço**
19	20	21	22	23	24	25	26	27

A mensagem a ser criptografada é a seguinte: **MATEMÁTICA E EDUCAÇÃO**.

1. Associamos cada letra do alfabeto e os espaços a um número e encontramos que o correspondente númerico de **MATEMÁTICA E EDUCAÇÃO** é 13 1 20 5 13 1 20 9 3 1 27 5 27 5 4 21 3 1 3 1 15 27.
2. Definimos a matriz codificadora e calculamos sua inversa, que será a chave.

$$A = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \; e \quad A^{-1} = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$$

3. Para codificar, definimos uma matriz B com os correspondentes numéricos da mensagem, que deverá ter a mesma quantidade de linhas da matriz A, e realizamos o produto $A \cdot B$.

$$A \cdot B = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 13 & 1 & 20 & 5 & 13 & 1 & 20 & 9 & 3 & 1 & 27 \\ 5 & 27 & 5 & 4 & 21 & 3 & 1 & 3 & 1 & 15 & 27 \end{pmatrix}$$

obtendo 31 29 45 14 47 5 41 21 7 7 81 49 57 70 23 81 9 62 33 11 13 135 como a mensagem codificada.

Ao receber a mensagem codificada o destinatário multiplica a matriz $A \cdot B$ pela chave A^{-1} (matriz inversa).

$$A^{-1} \cdot (A \cdot B) = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 31 & 29 & 45 & 14 & 47 & 5 & 41 & 21 & 7 & 17 & 81 \\ 49 & 57 & 70 & 23 & 81 & 9 & 62 & 33 & 11 & 33 & 135 \end{pmatrix}$$

e obtém-se a sequência numérica 13 1 20 5 13 1 20 9 3 1 27 5 27 5 4 21 3 1 3 1 15 27, que ao substituir os números encontrados pelas letras correspondentes de acordo com a Tabela 4.1 encontra-se a mensagem original: **MATEMÁTICA E EDUCAÇÃO**.

A segunda técnica é a cifra de Hill a qual possui dois aspectos distintos da primeira: divide a mensagem a ser cifrada em blocos e utiliza da Aritmética Modular, como apresentaremos a seguir.

4.1 Cifra de Hill

A cifra de Hill,um sistema de criptografia polialfabético de chave simétrica, que tem embasamento teórico nas operações matriciais e na aritmética modular.

Para criptografar uma mensagem utilizando a Cifra de Hill, associamos cada letra do texto a ser cifrado ao seu valor numérico de acordo com a Tabela 4.2, na qual o valor numérico do Z é 0, pois usaremos aritmética módulo 26.

Em seguida escolhemos uma matriz A de ordem $n \times n$ com entradas inteiras e que admita

Tabela 4.2: Alfabeto com o seu respectivos valores numéricos

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

inversa

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Agrupamos letras sucessivas do texto a ser cifrado em n-uplas, substituindo cada letra do texto pelo seu valor numérico encontrado na Tabela 4.2.

Convertemos cada n-upla sucessiva $p_1 p_2 ... p_n$ do texto a ser cifrado em um vetor coluna, substituindo os inteiros maiores que 25 pelo resto da divisão por 26.

$$P = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}$$

e obtemos o produto $A \cdot p$

$$A \cdot p = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}$$

Chamamos p de vetor coluna e $A \cdot p$ o vetor cifrado Feito isso, convertemos cada vetor cifrado em seu equivalente alfabético utilizando a Tabela 4.2.

4.1.1 Codificando uma Mensagem

Para codificar a palavra **CONEDU**.

1. Escolhemos a matriz codificadora de ordem 2

$$A = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}$$

2. Formamos um vetor coluna com cada par de letras (CO NE DU), substituindo cada letra pelo seu valor numérico de acordo com a Tabela 4.2.

$$CO \Rightarrow p = \begin{pmatrix} 3 \\ 15 \end{pmatrix} \qquad NE \Rightarrow p = \begin{pmatrix} 14 \\ 5 \end{pmatrix} \qquad DU \Rightarrow p = \begin{pmatrix} 4 \\ 21 \end{pmatrix}$$

3. Multiplicamos a matriz A pelo vetor coluna p, substituindo os valores maiores que 25 pelo resto da divisão por 26 e encontramos a matriz codificada.

$$CO \Rightarrow A \cdot p = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 15 \end{pmatrix} = \begin{pmatrix} 13 \\ 15 \end{pmatrix} \quad NE \Rightarrow A \cdot p = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 5 \end{pmatrix}$$

$$DU \Rightarrow A \cdot p = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 21 \end{pmatrix} = \begin{pmatrix} 2 \\ 21 \end{pmatrix}$$

Assim, obtemos 13 15 0 5 2 21 e substituindo cada número pelo seu correspondente alfabético, a mensagem criptografada é **MOZEBU**

4.1.2 Decodificando uma Mensagem

Temos a mensagem cifrada **MOZEBU**

1. Recorremos a Aritmética Modular para encontrar a matriz inversa de A e obtemos

$$A^{-1} = \begin{pmatrix} 9 & 8 \\ 0 & 1 \end{pmatrix}$$

2. Pela Tabela, **MOZEBU** corresponde a 13 15 0 5 2 21.

$$MO \Rightarrow p = \begin{pmatrix} 13 \\ 15 \end{pmatrix} \qquad ZE \Rightarrow p = \begin{pmatrix} 0 \\ 5 \end{pmatrix} \qquad BU \Rightarrow p = \begin{pmatrix} 2 \\ 21 \end{pmatrix}$$

3. Multiplicamos a matriz A^{-1} pelo vetor coluna p, substituindo os valores maiores que 25 pelo resto da divisão por 26 e encontramos a mensagem original.

$$MO \Rightarrow A^{-1} \cdot p = \begin{pmatrix} 9 & 8 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 13 \\ 15 \end{pmatrix} = \begin{pmatrix} 3 \\ 15 \end{pmatrix} \quad ZE \Rightarrow A^{-1} \cdot p = \begin{pmatrix} 9 & 8 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 5 \end{pmatrix} = \begin{pmatrix} 14 \\ 5 \end{pmatrix}$$

$$BU \Rightarrow A^{-1} \cdot p = \begin{pmatrix} 9 & 8 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 21 \end{pmatrix} = \begin{pmatrix} 4 \\ 21 \end{pmatrix}$$

Encontramos os valores 3 15 14 5 4 21 que na Tabela 4.2 correspondem a **CONEDU**.

5 Sequência Didática

Podemos definir sequência didática como um conjunto de atividades desenvolvidas para ensinar um determinado assunto associando-o com outros temas, tornando o conhecimento lógico. As atividades de uma sequência didática são planejadas visando alcançar os objetivos traçados

pelo professor. Para Zabala (1998, p.18) sequências didáticas são "um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim conhecidos tanto pelos professores como pelos alunos".

Nesse sentido, apresentaremos a seguir uma sequência didática desenvolvida a partir do estudo bibliográfico sobre criptografia e os conteúdos matemáticos que fundamentam essa técnica. Esse procedimento metodológico está direcionado para o ensino de matrizes na Educação Básica a partir da Cifra de Hill. A sequência didática está dividida em cinco momentos com seus respectivos cronograma de duração.

1º Momento: Apresentação do tema

Inicialmente recomenda-se que o professor aborde sobre o que é a criptografia e os seus aspectos históricos, evidenciando a necessidade dessa técnica nos dias atuais. Esse momento é interessante para despertar a curiosidade dos alunos a respeito do tema, podendo utilizar vários recursos didáticos para a aula inclusive do meio tecnológico. Em seguida, recomenda-se que o professor peça para que os alunos realizem uma pesquisa sobre os conteúdos matemáticos que estão presentes na criptografia. Para a realização desse momento serão necessárias 3 aulas.

2º Momento: Abordagem dos conteúdos matemáticos presentes na criptografia

Nesse momento, os alunos já teriam realizado a pesquisa sobre quais conteúdos matemáticos estão presentes na criptografia, então o professor poderá iniciar um debate sobre a pesquisa realizada, evidenciando como uma mensagem pode ser codificada através das operações matriciais. Para a realização desse momento serão necessárias 2 aulas.

3º Momento: Delimitação da cifra e do conteúdo matemático a ser estudado

Nesse momento o professor explicará sobre a cifra escolhida, abordando os conteúdos matemáticos que são utilizados para cifrar e decifrar uma mensagem através dessa cifra. Em seguida, o professor explicará o conteúdo de matriz e suas definições, como abordamos na Seção 3 deste trabalho. E deve introduzir o conceito de congruência. Uma proposta para explicar congruência de uma forma mais simples, seria explicar utilizando apenas como o resto da divisão. Para a realização desse momento serão necessárias 8 aulas.

4º Momento: Atividade realizada pelo professor

Aqui o professor trará uma atividade para ser realizada juntamente com os alunos em sala, nessa atividade o objetivo será cifrar e decifrar a mensagem utilizando os conceitos matemáticos adquiridos anteriormente. Para a realização desse momento serão necessárias 3 aulas.

5º Momento: Atividade realizada pelos alunos

Nessa fase final o professor deixa que os alunos façam outra atividade para cifrar e decifrar a mensagem, fazendo com que eles apliquem toda a teoria aprendida para solucionar a atividade. Eles devem escolher sua própria chave de codificação e decodificação aplicando conceitos de matriz inversa, multiplicação entre matrizes, entre outros. O professor deve observar quais procedimentos e estratégias foram utilizadas pelos alunos. Para a realização desse momento

serão necessárias 3 aulas.

6 Conclusões

Assim, conclui-se que a criptografia como uma área tecnológica e atual, pode subsidiar os professores da Educação Básica no ensino de matrizes. Visto que a criptografia por ter um vasto campo conceitual e histórico, pode ser trabalhada em sala de aula de várias formas como uma aplicação de conteúdos matemáticos, mostrando assim a importância e as aplicações da Matemática.

Para trabalho futuro pode-se estudar algum outro método criptográfico para abordar em sala de aula, uma vez que a criptografia está embasada teoricamente pela matemática, também pode-se estudar a utilização de recursos tecnológicos desenvolvendo um programa ou aplicativo para criptografar e descriptografar, no qual, o mesmo possa auxiliar o professor no ensino dos conteúdos matemáticos presentes no método criptográfico abordado.

7 Referência

CHAVANTE, E. PRESTES, D. **Quadrante matemática, 2º ano: ensino médio**. São Paulo, SP. 1ª ed. Edições SM, 2016.

IEZZI, G. HAZZAN, S. **Fundamentos de Matemática Elementar**. São Paulo, SP. 2ª ed., vol.4. Atual Editora, 1977.

JESUS, A. L. N. **Criptografia na Educação Básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes**. 2013. 82 f. Dissertação(Mestrado Profissional em Rede em Matemática)- Universidade Federal do Vale do São Francisco, Juazeiro, Bahia.

JESUS, A. L. N. **Criptografia na Educação Básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes**. 2013. 82 f. Dissertação(Mestrado Profissional em Rede em Matemática)- Universidade Federal do Vale do São Francisco, Juazeiro, Bahia.

OLGIN, C.A., GROENWALD, C. L. O.**Criptografia e conteúdos de Matemática do Ensino Médio**. II CNEM- Congresso Nacional de Educação Matemática, 2011.

SANTOS, J. P.O. **Introdução à Teoria dos Números**. Rio de Janeiro, RJ. 3ª ed., Coleção matemática universitária. Instituto de Matemática Pura e Aplicada-IMPA, 2014.

SINGH, S.**O livro dos Códigos**. Cidade. 1ª ed., Record, 2001.

TRIVINOS, A. N. S.. **Introdução a pesquisa em ciências sociais: a pesquisa qualitativa em educação**. São Paulo: Atlas, 1987.

ZABALA, ANTONI **A prática educativa: como ensinar**. Porto Alegre: Artmed, 1998.