VI EnGEM
Encontro Goiano de Educação Matemática
De 4 a 6 de maio de 2017
Instituto Federal de Educação, Ciência e Tecnologia Goiano - Campus Urutaí
ISSN: 2176-3305

UMA FERRAMENTA DE ENSINO DE MATRIZES UTILIZANDO A CRIPTOGRAFIA

Tatiane de Andrade Resende[1]

RESUMO

O presente trabalho se encontra em andamento no Curso de Especialização em Ensino de Ciências e Matemática no Instituto Federal Goiano- Campus Morrinhos- Goiás. O trabalho consiste em abordar uma metodologia didática para o ensino de Matrizes apresentada no Currículo Referência de Matemática do Ensino Médio do Estado de Goiás. O Currículo Referência tem como propósito colaborar com as Unidades Educacionais proporcionando propostas de bimestralização dos conteúdos para melhor compreensão dos componentes do currículo e sua utilização na sala de aula, ou seja, busca-se referenciar uma base comum essencial a todos estudantes, em consonância com as atuais necessidades de ensino identificadas não somente nas legislações vigentes, Diretrizes e Parâmetros Curriculares Nacionais, mas também nas matrizes de referências dos exames nacionais e estaduais, bem como a matriz curricular. Com o auxílio da Criptografia este trabalho trará contribuição para o ensino de Matemática, pois permite que o professor desenvolva atividades didáticas de codificação e decodificação para introduzir, revisar ou até mesmo aprofundar conteúdos matemáticos despertando o interesse do aluno e com isso estimulando a curiosidade que desencadeiem um processo cognitivo e permite a construção de novos conhecimentos. A escola na qual será aplicada o trabalho é uma Escola Pública Estadual com alunos do 2º ano do Ensino Médio no turno vespertino. Segundo Tamarozzi (2001), o tema Criptografia possibilita o desenvolvimento de atividades didáticas envolvendo o conteúdo de funções e matrizes que se constituem em material útil para exercícios, atividades e jogos de codificação, onde o professor pode utilizá-los para fixação de conteúdo. Nesse sentindo, este trabalho apresenta como objetivo uma alternativa educacional como uma ferramenta pedagógica que abrange os conteúdos matemáticos para propor aulas de matemáticas mais instigante e desafiadora**.**

Palavras-chave: Criptografia; Educação Matemática; Matrizes.

1 INTRODUÇÃO

Este projeto de pesquisa ainda em desenvolvimento aborda uma importância significativa no ensino aprendizagem da Matemática da Educação Básica, pois tem como

[1] Universidade Estadual de Goiás. E-mail: tateresende@hotmail.com

intuito apresentar uma ferramenta didática com o tema Criptografia para o ensino da Matemática do Ensino médio, especificamente no conteúdo de Matrizes, proporcionando uma alternativa educacional diversificada e tornando as aulas de Matemática mais desafiadoras.

A criptografia são artifícios para ocultação de mensagens. Há tempos atrás líderes de grandes nações questionavam seus súditos em busca de técnicas eficientes para proteção de mensagens confidenciais, a fim de traçar planos de guerra sem que suas mensagens caíssem em mão erradas. A busca por uma técnica segura tomava preocupação, já que os meios tecnológicos eram preexistente naquele período. Neste período era utilizado a esteganografia, que era simplesmente a ocultação das mensagens, porém não trazia segurança, pois se o mensageiro fosse descoberto, o inimigo descobriria a mensagem. Foi somente com a Segunda Guerra Mundial que a comunicação secreta ganhou impulso. Surge então a criptografia, que junto com a esteganografia tornou- se eficiente, pois dada a esteganografia ocultação de mensagens e a criptografia que é a substituição de palavras ou frases por símbolos, torna a mensagem mais complicada de ser descoberta.

O desejo em proteger mensagens confidenciais teve início há milhares de anos atrás. Grandes líderes recorriam de comunicações eficientes para comandar seus exércitos, com intuito de seus segredos valiosos não pudessem ser burlados pelos seus inimigos. Conforme Singh (2003) cita, os antigos chineses escreviam suas mensagens em seda fina, onde era amassada e em seguida coberta com cera, consequentemente engolida pelo mensageiro e cuspida ao chegar a seu destino.

Há indícios que os primeiros relatos de escritas secretas foram mencionadas por Heródoto, um grande filósofo grego, que ditou os conflitos entre Grécia e Pérsia. A partir de então considerado “o pai da história”. Heródoto revelou que foi graças à escrita escondida que livrou a Grécia de ser conquista por Xerxes, Reis dos Reis. Compondo como personagem principal Demarato, que por inadimplência com Xerxes havia revelado seu ataque à Grécia. Demarato sobrevivia sobre os vilarejos de persa de Susa, após ter sido expulsado da sua cidade natal Grécia. Por conta disso e exprimindo lealdade a sua naturalidade decidiu mandar um aviso para Grécia comunicando sobre o ataque surpresa que Xerxes estava planejando. Para manter tal sigilo sem que os guardas tomasse poder da mensagem, raspou a cera de um par de tabuletas de madeira, escreveu a suposta mensagem e cobriu novamente com cera. Com isso a escrita escondida passou a dominar

os tempos remotos e ser uma grande alternativa para se manter sigilo entre mensagens confidenciais.

Uma das fascinantes histórias citadas por Heródoto tem-se a história de Histaeu, que por sua vez queria incentivar Aristágora de Mileto a sublevar-se contra o rei persa. Como veremos na citação de Singh (2003):

> Para transmitir suas instruções em segurança, Histaeu raspou a cabeça do mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo voltasse a crescer. Evidentemente, aquele foi um período da história que tolerava uma certa falta de pressa. O mensageiro, que aparentemente não levava nada que fosse perigoso, pôde viajar sem ser incomodado. Quando chegou ao seu destino, raspou a cabeça e a virou para o destinatário da mensagem (SINGH, 2003, p. 21).

Notavelmente, observa-se a demora da entrega de uma mensagem naquele período. Os egípcios e romanos utilizavam a escrita escondida para comunicação de planos de guerra, mas somente com a 2ª Guerra Mundial que a comunicação escrita tomou impulso. Desde então, a esteganografia se tornou presente em nosso cotidiano.

Com o auxílio da Era da Informática a ciência da criptografia tornou-se mais potente, porém as pessoas não autorizadas também se beneficiaram com as tecnologias passando a criar fontes poderosas para quebrar os devidos códigos.

Então, fez-se necessário a utilização de métodos cada vez mais fortes e inquebráveis. Devido a isso a Matemática, uma ciência ampla, especificamente com a utilização da Álgebra Linear e Teoria dos Números, se tornou extremamente importante, que por sua vez ainda fez uma conexão com o poder computacional impulsionando o estudo da criptografia, resultando em códigos mais robustos e seguros. O estudo da álgebra linear e teoria dos números recorrem a algoritmos mais complexos e abstratos, contribuindo de forma eficiente na ligação com a criptografia.

Com a utilização de matrizes pretende-se fornecer um meio seguro e efetivo para trocas de mensagens. Assim, com a utilização desta técnica de forma adequada pretende-se garantir mais confiabilidade nos dados que serão trafegados, dificultando ainda mais o trabalho de ataque de pessoas não autorizadas.

É notável que o interesse do aluno é evidenciado pelo concreto e pelas intervenções simples com dinâmicas. De acordo com Tamarozzi (2001), o tema Criptografia possibilita o desenvolvimento de atividades didáticas envolvendo o conteúdo de funções e matrizes que se constituem em material útil para exercícios, atividades e jogos de codificação, onde o professor pode utiliza-los para fixação de conteúdo. Este trabalho aborda uma importância significativa no ensino aprendizagem da Matemática da

Educação Básica, pois tem como intuito apresentar uma ferramenta didática com o tema Criptografia para o ensino da Matemática do Ensino Médio, proporcionando uma alternativa educacional diversificada e tornando as aulas de Matemática mais desafiadoras.

2. METODOLOGIA

A pesquisa apresenta um levantamento bibliográfico acerca das produções sobre criptografia, além dessas leituras, está sendo realizada estudos que propiciem a realização de uma contextualização da Educação Matemática na Educação Básica. É notável que a aprendizagem dos conteúdos de Matemáticas apresentam muitas maneiras de se aprender. Concordando com Duval (2003), acredita-se que desta forma, os conteúdos apresentados não serão simplesmente fixados pelos alunos, mais sim que possamos fazer com que este aluno considere as aulas de matemática mais desafiadoras. O uso de Criptografia durante as aulas se faz interessante, pois permite que o professor desenvolva atividades didáticas que adaptem as aulas e despertem a atenção e o interesse dos alunos para os conteúdos trabalhados em sala de aula.

O trabalho é constituído em duas partes. A primeira desenvolvida através de um levantamento bibliográfico em torno das considerações de Criptografia e do desenvolvimento de atividades didáticas para o Currículo de Matemática do Ensino Médio.

A segunda parte será o desenvolvimento de um experimento constituído por uma divisão de grupos. No início do experimento será realizado um questionário, com 38 alunos do 2º ano, do Ensino Médio, em uma Escola Estadual situada no Município de Morrinhos, Goiás. As atividades serão realizadas em oito horas/aula, distribuídas em três dias letivos referente ao segundo bimestre. Com base no currículo de referência o aluno do 2º ano do Ensino Médio deve apresentar conhecimento em matrizes, pois no currículo se encontra no primeiro bimestre. O conteúdo que será proposto será*: Operações de Matrizes*. Os dados obtidos serão coletados através da observação e da análise dos registros dos mesmos. Finalizaremos, com a colhida das opiniões dos alunos em relação a atividades propostas.

2.1 ATIVIDADE PROPOSTA COMO ALTERNATIVA EDUCACIONAL: CÓDIGO COM MULTIPLICAÇÃO DE MATRIZES

Depois da leitura e do estudo da história da escrita escondida, será apresentada a atividade com o uso de códigos para que os alunos conheçam os conceitos básicos de Criptografia, conforme a seguir:

Como exemplo utilizaremos a palavra **TRABALHO.**

1º Passo: É codificar a mensagem, com isso decorremos da notação alfabética para a notação numérica, neste caso a utilização da Cifra de Hill.

Quadro 1 – Quadro com a Cifra de Hill

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

Observação: Notamos que o alfabeto compõe por 26 letras, a Cifra de Hill estabelece a ordem numérica com exceção do zero que substitui a letra Z.

2º Passo: Seleciona-se a uma matriz de ordem *n* que denominada de Matriz Codificadora, que será a chave do ciframento. No entanto, é imprescindível, que ela tenha inversa. Como exemplo, será utilizada a seguinte matriz de ordem 2.

$$A_{2X2} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

3º Passo: Seleciona-se a mensagem, por exemplo: **TRABALHO.** Adiante, agrupa-se o texto em pares de letras[10] e realiza a conversão através do quadro:

T	R	A	B	A	L	H	O
20	18	1	2	1	12	8	15

4º Passo: Cada par de números deve ser convertido em um vetor coluna. Cada vetor coluna será multiplicado pela matriz codificadora, então:

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 18 \end{bmatrix} = \begin{bmatrix} 56 \\ 18 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 12 \end{bmatrix} = \begin{bmatrix} 25 \\ 12 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 15 \end{bmatrix} = \begin{bmatrix} 38 \\ 15 \end{bmatrix}$$

5º Passo: Faz-se a conversão dos valores encontrados de acordo com o quadro. Como podemos notar no exemplo acima, existem alguns valores que não possuem correspondente no quadro.

Sempre que isso ocorrer como neste caso, é necessário aplicar a aritmética modular. Quando o resultado obtido for maior que 25, ele será substituído pelo resto da divisão desse número por 26. É por essa razão que a letra Z assume valor 0 no quadro. Então:

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 20 \\ 18 \end{bmatrix} \begin{bmatrix} 56 \\ 18 \end{bmatrix} \quad \begin{bmatrix} 4 \\ 18 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \end{bmatrix} \begin{bmatrix} 5 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 12 \end{bmatrix} \begin{bmatrix} 25 \\ 12 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 8 \\ 15 \end{bmatrix} \begin{bmatrix} 38 \\ 15 \end{bmatrix} \quad \begin{bmatrix} 12 \\ 15 \end{bmatrix} \pmod{26}$$

Pode ser visto no resultado acima, e procurando símbolo no quadro, obtemos:

4	18	5	2	25	12	12	15
D	R	E	B	Y	L	L	O

Obtém –se a seguinte mensagem: **DREBYLLO**

Para decifrar a mensagem obtida seguem-se os seguintes passos:

1º Passo: Obtém-se a inversa da matriz codificadora, que será a chave para decifrar o texto cifrado, denominada como Matriz Decoficadora.

Utilizando o método da matriz adjunta: $A^{-1} = \frac{1}{|A|} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (\text{mod } 26)$. Dada a matriz quadrada $A_{(2\times 2)} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \rightarrow |A| = (1 \cdot 1) - (2 \cdot 0) \rightarrow (1 - 0) = 1$. Então:

$$A^{-1} = \frac{1}{|A|} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad (\text{mod } 26)$$

$$A^{-1} = \frac{1}{1} \cdot \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \quad (\text{mod } 26)$$

$$A^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \quad (\text{mod } 26)$$

Portanto, a matriz decodificadora é:

$$D = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$$

2º Passo: Adiante agrupa-se o texto cifrado em pares de letras, e faz-se a conversão de acordo com o quadro:

D R E B Y L L O 4 18 5 2

25 12 12 15

3º Passo: Cada par de números deve ser convertido em um vetor coluna. Cada vetor coluna criado será multiplicado pela matriz decodificadora, e quando valor obtido for maior do que 25- aplica-se a aritmética módulo 26:

$$A^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 18 \end{bmatrix} = \begin{bmatrix} -32 \\ 18 \end{bmatrix} \rightarrow \begin{bmatrix} 20 \\ 18 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 25 \\ 12 \end{bmatrix} = \begin{bmatrix} 1 \\ 12 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 15 \end{bmatrix} = \begin{bmatrix} -18 \\ 15 \end{bmatrix} = \begin{bmatrix} 8 \\ 0 \end{bmatrix}$$

Observação: Nos cálculos acima se obteve dois sinais negativos -32 e -18, na aritmética modular faz-se o processo para torna-los positivos, pois não temos valores negativos no quadro da Cifra de Hill. Então:

5º Passo: Por fim, faz-se a conversão dos valores encontrados de acordo com o quadro:

20	18	1	2	1	12	8	0
T	R	A	B	A	L	H	O

Retornou- se, então, a mensagem original: **TRABALHO**.

Temos então a matriz codificada, ou ainda a mensagem codificada. Para a codificação, descobrir se o aluno realizou a tarefa corretamente ou ainda para verificação de aprendizagem, basta fazer a multiplicação da matriz pela inversa, ou seja, AM x A^{-1}. Dessa forma vimos quão grande a importância das matrizes inversas para a criptografia e ainda um excelente assunto para ser abordado nas aulas.

3 RESULTADOS ESPERADOS

Com a aplicação desta atividade pretende-se observar a interação de todos os alunos e o processo de socialização entre os grupos. Ainda, neste trabalho espera- se analisar que a codificação e a decodificação auxiliam de forma positiva nas aulas de Matemática. Esses artifícios despertam a atenção e o interesse dos alunos tornando as aulas mais produtivas resultando numa melhor compreensão do conteúdo, concentração, desenvolver estratégias para resoluções de problemas e trabalho em grupo. Com a aplicação da Criptografia este trabalho contribuirá para as aulas de Matemática, pois permite que o professor desenvolva atividades didáticas de codificação e decodificação para introduzir, revisar ou até mesmo aprofundar conteúdos matemáticos despertando o interesse do aluno e com isso estimulando a curiosidade que desencadeiem um processo cognitivo e permite a construção de novos conhecimentos

4 Referências

BRASIL. Ministério da Educação. Secretaria de Educação Básica. Secretaria de Educação Continuada, Alfabetização, Diversidade e Inclusão. Secretaria de Educação Profissional e Tecnológica. Conselho Nacional da Educação. Câmara Nacional de Educação Básica. **Diretrizes Curriculares Nacionais Gerais para a Educação Básica**. Brasília: MEC / SEB / DICEI, 2013. 562p.

DUVAL, R. **Aprendizagem em Matemática: r**egistros de representação semiótica. Campinas: Papirus, 2003.

BRASIL, Secretaria de Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais.** Ministério da Educação e cultura.Brasília: MEC, 2003.

SHOKRANIAN, S. **Criptografia para iniciantes**. Brasília: UnB, 2005.

SINGH, S.**O livro dos códigos**. 3. ed. Rio de Janeiro: Record, 2003.

TAMAROZZI, A. C. Codificando e decifrando mensagens. **Revista do Professor de Matemática**. São Paulo. n 45. 2001.