UNIVERSIDADE FEDERAL DE SÃO JOÃO DEL-REI – UFSJ
NÚCLEO DE EDUCAÇÃO À DISTÂNCIA
DEPARTAMENTO DE MATEMÁTICA E ESTATÍSTICA – DEMAT

Érica Maria Troiano da Silva

CAÇA AO TESOURO ATRAVÉS DA CRIPTOGRAFIA E MULTIPLICAÇÃO DE MATRIZES: UMA PRÁTICA NO ENSINO MÉDIO

SÃO JOÃO DEL-REI
2016
Érica Maria Troiano da Silva

CAÇA AO TESOURO ATRAVÉS DA CRIPTOGRAFIA E MULTIPLICAÇÃO DE MATRIZES: UMA PRÁTICA NO ENSINO MÉDIO

Trabalho de conclusão de curso, apresentado como requisito parcial para obtenção do título de Licenciado em Matemática, do curso de Licenciatura em Matemática a Distância, da Universidade Federal de São João Del-Rei.

Orientador: Carlos Alberto Raposo da Cunha

SÃO JOÃO DEL-REI

2016

Érica Maria Troiano da Silva

CAÇA AO TESOURO ATRAVÉS DA CRIPTOGRAFIA E MULTIPLICAÇÃO DE MATRIZES: UMA PRÁTICA NO ENSINO MÉDIO

.

Trabalho de conclusão de curso, apresentado como requisito parcial para obtenção do título de Licenciado em Matemática, do curso de Licenciatura em Matemática a Distância, da Universidade Federal de São João Del-Rei.

Os componentes da banca de avaliação, abaixo identificados, consideram este trabalho aprovado.

BANCA EXAMINADORA

_____

Prof.ª Dr. (nome)

(instituição)

_____

Prof.º Dr. (nome)

(Instituição)

Data da aprovação: São João del-Rei, ____ de _____ de _____.

RESUMO

Na atualidade, o docente em sua prática deve procurar métodos que envolvam os discentes e desperte o interesse pelos estudos. Sendo assim, neste trabalho apresento uma prática que utiliza a criptografia, na codificação e decodificação de mensagens através da multiplicação de matrizes.

Inicialmente é abordada a parte histórica da criptografia e os principais acontecimentos. Também é descrito sobre a definição de matrizes, as operações com matrizes e a matriz inversível.

Os próximos capítulos serão dedicados ao relato da prática realizada nas 2ªs séries do Ensino Médio da Escola Estadual Professor Roberto Scarabuci e por fim será dada a conclusão do trabalho.

Palavras-chave: Criptografia, codificação, decodificação .

ABSTRACT

Currently, teachers in their practice should look for methods that involve students and awaken the interest in studies. Thus, this paper present a practice that uses encryption, the encryption and decryption of messages using the matrix multiplication.

Initially covered is the historical part of the encryption and key events. It is also described on the definition of matrices, matrix operations, and invertible matrix.

The next chapters will be devoted to reporting the practice performed in 2ªs series of high school at the State School Professor Roberto Scarabuci and finally will be given to completion of the work.

Keywords: Encryption, encoding, decoding.

SUMÁRIO

1- INTRODUÇÃO

No atual cenário da educação, as aulas devem de alguma maneira fugir um pouco do tradicional, e despertar no estudante o interesse e a vontade de aprender.

Diante desses fatos o presente trabalho pretende aplicar uma pratica em sala de aula que envolve a codificação e decodificação de mensagens através da multiplicação de matrizes.

Para codificação das mensagens utilizaremos a criptografia, que tem por objetivo proteger o sigilo das mensagens. Para conhecimento da importância da criptografia e um pouco da parte história será apresentado o vídeo "Tempos Modernos" que mostra um pouco sobre o processo e conta um pouco da história dos criptonalistas nos tempos da guerra.

Ainda para maior incentivo dos alunos, será oferecido a eles um "tesouro" após a decifragem da mensagem que faz referência ao esconderijo.

Ao final do trabalho, esperamos a compreensão do método de multiplicação de matrizes e o envolvimento e participação dos estudantes no processo de aprendizagem de uma forma diferente e agradável.

2- A HISTÓRIA DA CRIPTOGRAFIA

2.1- **O código de César**

Uma das cifras mais conhecidas e usadas até hoje é o código de César (também conhecido como cifra de César), pelo qual as letras são trocadas por letras posicionadas três posições à frente, como representado na tabela 1, (NASCIMENTO, 2011).

Figura 1 – Código de César

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

Fonte: http://recantododragao.xpg.uol.com.br/2013/04/30/um-pouco-sobre-criptografia/

Observando este método notamos que a chave deve ser previamente combinada entre o emissor e o receptor da mensagem através de um meio sigiloso, além disso, deve ser mantida em segredo para evitar que uma pessoa não autorizada consiga ler a mensagem.

Apesar da sua simplicidade (ou exatamente devido a ela), esta cifra foi utilizada pelos sulistas na guerra de secessão americana e pelo exército russo em 1915, (TKOTZ,2005).

2.2- Criptonalistas Arábes

Criptoanálise é a ciência de quebrar uma mensagem cifrada. Veja bem, quebrar não é o mesmo que decifrar. Decifrar é obter a mensagem original quando se conhece o sistema e usando a chave também conhecida. Quebrar é hackear o sistema e descobrir a chave, (TKOTZ, 2005).

No século IX um matemático árabe, que trabalhava na "Casa da sabedoria de Bagdá", escreveu um livro manuscrito sobre o deciframento de mensagens criptográficas, (ARINOS, 2014).

Conhecido como Al-Kindi, seu maior trabalho só foi descoberto em 1987, no arquivo Otomano Sulaiyyah em Istambul, e se intitula: "Um manuscrito sobre a decifração de mensagens criptográficas". Nesse livro é descrito o método da analise das frequências, o qual permite "romper" todas as cifras de substituição monoalfabéticas, ou seja, cifras de substituição a partir das quais cada letra do texto claro é substituída por outra letra no texto cifrado, de forma constante, (ARINOS, 2014).

Al-Kindi foi o primeiro a estudar a frequência da letra nos idiomas mais conhecidos. Seu método consiste em decifrar uma mensagem codificada, quando se conhece o idioma, e para isso deve-se encontrar um texto diferente, na mesma língua, suficientemente longo para preencher uma pagina e fazer essa analise das frequências. A letra que aparecer com maior frequência é chamada de “primeira” a segunda mais frequente recebe o nome de “segunda” e assim por diante, até todas as letras serem contadas. Em seguida, examina-se o texto cujo deciframento será feito e os símbolos também são classificados com relação a frequência . O símbolo que aparecer com maior frequência é substituído pela “primeira”, o segundo mais frequente é substituído pela “segunda” e assim por diante, até todos os símbolos serem convertidos, (ARINOS, 2014).

2.3 - As cifras monoalfabeticas e polialfabeticas

Segundo Tkotz (2005) o sistema que substitui cada um dos caracteres de um texto claro usando outros caracteres (letras, números, símbolos, etc.) conforme uma tabela de substituição pré estabelecida é o sistema mais antigo que se conhece. As tabelas de substituição contem os caracteres que serão substituídos e os caracteres de substituição. Estas tabelas também são conhecidas como cifrantes ou alfabetos cifrantes. Quando apenas um cifrante é aplicado, a substituição é chamada de monoalfabética.

Sendo assim, houve um período na história que era necessário uma cifra mais resistente aos criptonalistas, e assim surgiram as substituições polialfabéticas que utilizavam mais de um cifrante para decodificação das mensagens.

Então o italiano Leon Batista Alberti criou a primeira cifra polialfabética.

O avanço principal do método de Alberti consiste em não permitir que a mesma letra do texto original apareça como única letra do alfabeto cifrado, ou seja, ele é o primeiro personagem que se tem noticia que utilizou a cifra de substituição polialfabética. Nesse método ele utilizava alternadamente dois alfabetos de César, causando uma enorme dificuldade para os criptonalistas, pois a analise das frequências era insuficiente para decifrar as mensagens, (ARINOS, 2014).

Outro personagem que utilizou o método da criptografia polialfabética foi o diplomata francês Blaise de Viqenêre. E para exemplificar sua técnica segue um exemplo utilizando o quadrado de Vigenêre:

Figura 2 – O quadrado de Vigenêre

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

Fonte:http://obviousmag.org/archives/2013/01/os_segredos_de_kryptos__a_escultura_misterio.html

Exemplo: Considere a palavra chave MATEMÁTICA para decifrar o texto TRABALHO DE CONCLUSÃO DE CURSO

As linhas do quadrado de Vigenêre a serem utilizadas são aquelas em que o alfabeto começa por M,A,T,E,M,A,T,I,C,A. Então a letra “T” será substituída pela letra correspondente no alfabeto que começa pela letra “M”, ou seja, a letra “F”. Depois a letra “R” será substituída pela letra correspondente no alfabeto que começa pela letra “A”, ou seja, a letra “R” e assim por diante até chegarmos ao texto cifrado.

2.4 - A cifragem através de máquinas

Segundo Singh (2007, p.13; apud Marques, 2013) a primeira máquina criptográfica que se tem registro foi inventada no século XV pelo arquiteto italiano Leon Alberti, um dos criadores da cifra polialfabética. A máquina era composta de dois discos de cobre. O maior era fixo e o menor era móvel. Cada disco continha o alfabeto ao longo da sua borda; no disco maior, o alfabeto original em letras maiúsculas e, no menor, o alfabeto cifrado em letras minúsculas.

Em 1918 o inventor alemão Arthur Scherbius e seu amigo Richar Ritter fundaram uma empresa, a Scherbius & Ritter. Um de seus projetos era substituir os sistemas de criptografia inadequados, usados na 1ª guerra mundial, a partir da troca de cifras de papel e lápis por uma forma de cifragem que usasse a tecnologia do século XX. Engenheiro eletricista de formação, ele patenteou uma invenção de uma máquina de cifra mecânica, basicamente uma versão elétrica do disco de Alberti, mais tarde vendida como a máquina Enigma, (MARQUES, 2013).

A enigma foi utilizada pelo exercito alemão durante a segunda guerra mundial, esta maquina foi utilizada como o método de comunicação mais seguro, pois seus usuários acreditavam que ela era indecifrável.

Sua fama durou até a primeira metade da década de 40, pois a partir do desenvolvimento e auxilio dos criptonalistas poloneses, o matemático Alan Turing consegui quebrar as cifras da enigma. Com isso o fim da 2ª guerra foi antecipado e muitas vidas foram poupadas.

Outro aparelho que tinha como finalidade decifrar mensagens foi desenvolvido na Inglaterra com base nas ideias de Turing. Denominado de “Colossos”, foi utilizado para decifrar as codificações feitas pela maquina Lorens, empregada nas comunicações de Hitler e seus generais, (ARINOS, 2014).

3 APLICAÇÃO DO PRODUTO DE MATRIZES

3.1 - Definição

De acordo com (Calliolli, 1998), sejam m≥1 e n≥1 dois números inteiros. Uma matriz m x n real é uma dupla sequência de números reais, distribuídos em m linhas e n colunas, formando uma tabela que se indica do seguinte modo:

Figura 2 – Representação da matriz

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ . & . & . & & . \\ . & . & . & & . \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

Fonte: o próprio autor

Assim,

a11 é o elemento da 1ª linha e 1ª coluna;

a32 é o elemento da 3ª linha e 2ª coluna

a23 é o elemento da 2ª linha e 3ª coluna, (PAES, 2014).

Ainda segundo Calliolo (1998) abreviadamente esta matriz pode ser expressa por (aij) 1 < i < m ou apenas 1 < j < n (aij), se não houver possibilidade de confusão quanto à variação dos índices.

Cada número que compõe uma matriz chama-se termo dessa matriz. Dada a matriz (aij) 1 < j < m, ao símbolo aij que representa indistintivamente todos os seus termos daremos o nome de termo geral dessa matriz.

Notações- Indicaremos por M_{mxn} (ℝ) o conjunto das matrizes reais m x n. Se m=n, ao invés de M_{nxn} (ℝ), usa-se a notação Mn (ℝ). Cada matriz de Mn (ℝ) chama-se matriz quadrada de ordem n. Em contraposição quando m ≠ n,

uma matriz m x n se diz a uma matriz retangular. Uma matriz 1 x 1 (a_{11}) se identifica com o número real a_{11}.

Cada matriz costuma ser denotada por uma letra maiúscula do nosso alfabeto.

Exemplo - A matriz

$$A=\begin{pmatrix} 1 & 0 \\ 1 & -3 \\ 0 & 4 \end{pmatrix}$$

é uma matriz real 3x2. Logo A ∈ M_{3x2} (ℝ).

Linhas e Colunas

Dada a matriz A=

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ . & . & . & & . \\ . & . & . & & . \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

As m sequências horizontais

$A^{(1)}= (a_{11}, a_{12}, \dots, a_{1n})$,..., $A^{(m)}= (a_{m1}, a_{m2}, \dots, a_{mn})$

são chamadas linhas da matriz A, enquanto que as n sequencias verticais

$$A(1)=\begin{pmatrix} a_{11} \\ a_{21} \\ \dots \\ a_{m1} \end{pmatrix} \quad ,\dots, \quad A(n)=\begin{pmatrix} a_{1n} \\ a_{2n} \\ \dots \\ a_{mn} \end{pmatrix}$$

São as colunas de A. É de se notar que cada $A^{(i)} \in M_{1xn}$ (ℝ) e cada $A_j \in M_{mx1}$ (ℝ).

Exemplo – na matriz 2x3

$$A=\begin{pmatrix} 1 & 0 & 1 \\ 0 & 6 & -5 \end{pmatrix}$$

As linhas são (1,0,1) e (0,6,-5) ao passo que as colunas são $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 6 \end{pmatrix}, \begin{pmatrix} 1 \\ -5 \end{pmatrix}$

Igualdade de matrizes

Consideremos duas matrizes reais mxn, A= (a_{ij}) e B= (b_{ij}). Dizemos que A=B se e somente se, $a_{ij} = b_{ij}$(i=1,2,...,m,j=1,2,...,n).

Exemplos:

1) $\begin{pmatrix} 1 & 2 & 1 \\ 0 & x & 0 \end{pmatrix} = \begin{pmatrix} y & 2 & z \\ t & -1 & 0 \end{pmatrix}$ $\leftrightarrow$ x = -1, y = 1, t = 0 e z = 1

2) $\begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 4 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 1 & 4 \end{pmatrix}$

3) $\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 3 \\ 0 & 0 & 0 \end{pmatrix}$

3.2 – Operações com matrizes

a) Adição

Sejam A= (a_{ij}) e B= (b_{ij}) matrizes mxn. Indicamos por A+B e chamamos soma de A com B a matriz mxn cujo termo geral é $a_{ij} + b_{ij}$, ou seja

$$A+B = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ \dots & & & \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

A operação que transforma cada par (A,B) de matrizes do mesmo tipo na matriz A+B chama-se adição de matrizes. É uma operação no conjunto M_{mxn} (ℝ).

Exemplo: Se $A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} e \quad B = \begin{pmatrix} 0 & 1 & -2 \\ 2 & 4 & 7 \end{pmatrix}$, então

$$A+B = \begin{pmatrix} 1 & 3 & -1 \\ 2 & 5 & 9 \end{pmatrix}$$

Para a adição de matrizes acima valem as seguintes propriedades:

I) A+ (B+C) = (A=B) +C, ∀ A, B, C ∈ M_{mxn} (ℝ) (associativa);

II) A+B= B+A, ∀ A,B ∈ M_{mxn} (ℝ) (comutativa);

III) Existe uma matriz 0 ∈ M_{mxn} (ℝ) (existe elemento neutro);

IV) Dada uma matriz A ∈ M_{mxn} (ℝ), existe uma matriz (-A), também mxn, tal que A+(-A) = 0 (existe a oposta de qualquer matriz).

A verificação da propriedade associativa se faz assim:

Se A= (a_{ij}), B= (b_{ij}) e C = (c_{ij}), então (A+B)+C = $(a_{ij} + b_{ij})+(c_{ij})$ = $((a_{ij}+b_{ij})+(c_{ij}))$ = $(a_{ij}+(b_{ij}+c_{ij}))$ = $(a_{ij})+(b_{ij}+c_{ij})$ = A+(B+C).

Quanto à (III) é fácil ver que: $0 = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & & & \\ 0 & 0 & \dots & 0 \end{pmatrix}$

Esta matriz chama-se matriz nula mxn. Por último, se A = (a_{ij}), é evidente que (-A) = (-A) = $(-a_{ij})$. Por exemplo, se $A = \begin{pmatrix} 1 & a & -2 \\ -2 & 1 & 0 \end{pmatrix}$, então –A = $\begin{pmatrix} -1 & -a & 2 \\ 2 & -1 & 0 \end{pmatrix}$

b) Multiplicação de uma matriz por um número

Dada uma matriz real A = (a_{ij}), mxn, e dado um número real $\propto$, o produto de $\propto$ por A é a matriz real mxn dada por:

$$\propto A = \begin{pmatrix} \propto a_{11} & \dots & \propto a_{1n} \\ \dots & \dots & \dots \\ \propto a_{m1} & \dots & \propto a_{mn} \end{pmatrix}$$

Para essa operação que transforma cada par ($\propto$, A) de $\mathbb{R}$ x M_{mxn} ($\mathbb{R}$) na matriz real $\propto$ A $\in$ M_{mxn} ($\mathbb{R}$), valem as seguintes propriedades:

I) $(\propto \beta)A = \propto (\beta A)$;

II) $(\propto + \beta)A = \propto A + \beta A$;

III) $\propto (A+B) = \propto A + \propto B$;

IV) $IA = A$;

Quaisquer que sejam as matrizes A e B e qualquer que seja os números $\propto$ e β.

Provemos (II),

Suponhamos A= (a_{ij}). Então:

$(\propto+\beta) . A = ((\propto+\beta). a_{ij}) = (\propto a_{ij} + \beta a_{ij}) = (\propto . a_{ij}) + (\beta . a_{ij}) = \propto A + \beta A$

Exemplo – Se $\propto = 2$ e $A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 4 \end{pmatrix}$, então $\propto A = \begin{pmatrix} 2 & 4 & 2 \\ 0 & 2 & 4 \\ 0 & 0 & 8 \end{pmatrix}$

c) Multiplicação de matrizes

Consideremos a matriz A =(a_{ij}) de tipo mxn e a matriz B =(b_{jk}) de tipo nxp. O produto A.B (também indicado por AB) é a matriz mxp cujo termo geral é dado por:

$C_{ik} = \sum_{j=1}^{n} a_{ij}.b_{jk} = a_{i1}.b_{jk} + \dots + a_{in}.b_{nk}$

Usando a notação de matriz linha e a de matriz coluna a definição acima significa que:

$$AB = \begin{pmatrix} A^{(1)}.B_1 & \dots & A^{(1)}.B_p \\ A^{(2)}.B_1 & \dots & A^{(2)}.B_p \\ \dots & \dots & \dots \\ A^{(m)}.B_1 & \dots & A^{(m)}.B_p \end{pmatrix}$$

Nas condições acima, a operação que transforme cada par de matrizes(A,B) na matriz AB chama-se multiplicação de matrizes.

Exemplo – Sejam $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$ e $B = \begin{pmatrix} 3 & 4 & 5 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

Então, $AB = \begin{pmatrix} 2.3+1.0+0.1 & 2.4+1.0+0.0 & 2.5+1.0+0.1 \\ 0.3+1.0+2.1 & 0.4+1.0+2.0 & 0.5+1.0.2.1 \end{pmatrix} = \begin{pmatrix} 6 & 8 & 10 \\ 2 & 0 & 2 \end{pmatrix}$

Proposição 2 – Sejam A=(a_{ij}), B = (b_{jk}) e C= (c_{ky}) matrizes reais m x n, n x p e p x q, respectivamente. Então A (BC) = (AB)C.

Demonstração – O termo geral de A (BC) é dado por

$$\sum_{j=1}^{n} a_{ij(\sum_{k=1}^{p} b_{jk}} \ c_{ky}) \qquad (1)$$

Ao passo que o termo geral AB é dado por:

$\sum_{k=1}^{n}(\sum_{j=1}^{n} a_{ij}\, b_{jk})\, c_{ky}$ (2)

As propriedades da adição e da multiplicação de números reais nos ensinam, contudo que (1) = (2). Então a proposição esta demonstrada.

Proposição 3 – Sejam A, B e C matrizes reais m x n, n x p e n x p, respectivamente. Então A (B+C) = AB+AC.

Demonsração – Usa-se o mesmo tipo sw raciocínio da demonstração anterior.

Nota: Analogamente, se A e B são matrizes m x n e C é n x p, então (A+B)C = AC+BC.

3.3 – Matrizes Inversíveis

Definição segundo Callioli (1998). Consideramos neste parágrafo apenas as matrizes quadradas de ordem n. Neste caso a multiplicação transforma cada par de matrizes de ordem n numa outra matriz, também de ordem n. E além das propriedades dadas pelas proposições 2 e 3 acima (associativa e distributiva em relação à adição) a multiplicação neste caso, goza da propriedade de admitir elemento neutro que é a matriz

$$In = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

e que evidentemente verifica as condições AIn = InA = A, para toda matriz A de ordem n. A matriz IN chama-se matriz identidade de ordem n.

Definição – Uma matriz A de ordem n se diz inversível se, e somente se, existe uma matriz B, também de ordem n, de modo que

AB = BA = In

Esta matriz B, caso exista,é única e chama-se inversa de A, indica-se por A^{-1}.

Exemplo: Caso exista, determine a inversa da matriz A = $\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$;

Consideremos B = A^{-1}= $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$;

$\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;

3.a + 2.b = 1

3.c + 2.d = 0

a + b = 0

c + d = 1

Resolvendo as equações temos que:

$\begin{cases} 3.a + 2.b = 1 \\ a + b = 0 \end{cases}$ $\begin{cases} 3.c + 2.d = 0 \\ c + d = 1 \end{cases}$

3.a + 2.b = 1

a + b = 0 (-2)

3a + 2b = 1

-2a - 2b = 0

a = 1

1 + b = 0

b = -1

3.c + 2.d = 0

c + d = 1 (-2)

3c + 2d = 0

-2c – 2d = -2

c = -2

c + d = 1

-2 + d = 1

d = 1+2 = 3

Assim, $\begin{pmatrix} 1 & -2 \\ -1 & 3 \end{pmatrix} = A^{-1}$

4 - UMA APLICAÇÃO DA CRIPTOGRAFIA NO ESTUDO DE MATRIZES EM SALA DE AULA

As atividades foram realizadas nas três turmas da 2ª série do Ensino Médio da E.E. Prof. Roberto Scarabuci, entre os dias 01 e 06 de junho do presente ano. Primeiramente os alunos da 2ª série A assistiram o vídeo "Tempos Modernos", que tem por objetivo mostrar a importância da criptografia na evolução histórica e tecnológica e com isso despertar o interesse dos estudantes para a atividade.

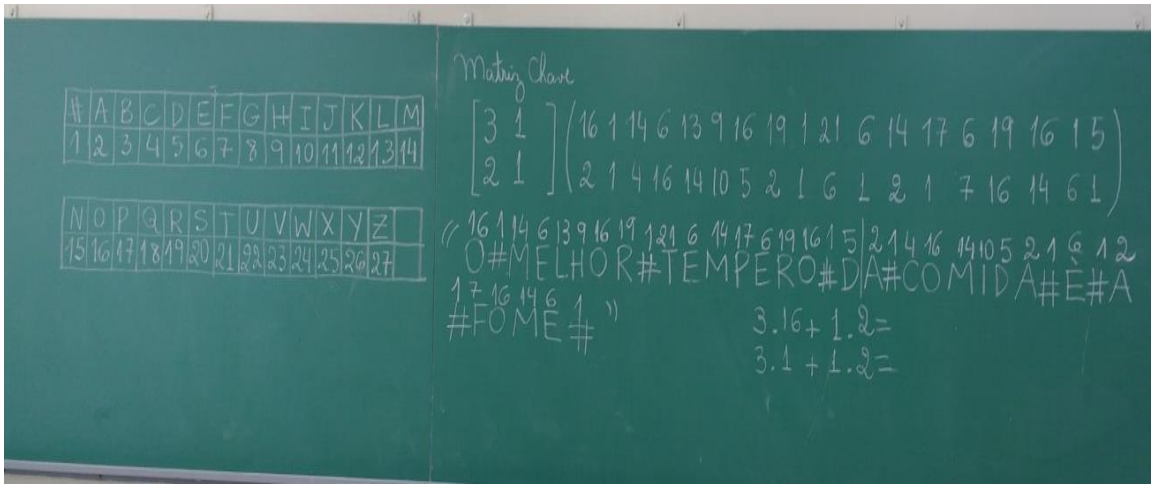
Posteriormente, na sala de aula foi revisado o conceito de matriz inversível através de um exemplo. Dando sequência a atividade, no quadro apresentei um alfabeto representado por números e solicitei que os alunos, em grupos, transformassem a mensagem "Informática o hardware da vida" numa matriz mensagem e depois multiplicassem esta matriz pela matriz chave dada por A = $\begin{matrix} 2 & 1 \\ 5 & 3 \end{matrix}$, codificando a mensagem.

Realizada a codificação pedi que os grupos colocassem a mensagem codificada para ser entregue a outra turma decodificar.

A próxima aula foi realizada na 2ª série C, e atividade foi realizada na mesma sequência, no entanto a mensagem a ser codificada foi " A leitura engrandece a alma" e a chave para codificação foi dada por A= $\begin{matrix} 2 & -5 \\ -1 & 3 \end{matrix}$.

Para a 2ª série B foi entregue a mensagem "O melhor tempero da comida é a fome" e a matriz chave A= $\begin{matrix} 3 & 1 \\ 2 & 1 \end{matrix}$.

Figura 3- Foto do alfabeto no quadro



Fonte: Próprio autor

Na próxima etapa da atividade, que também teve inicio na 2ª série A, entreguei aos grupos a folha com a mensagem codificada pelos grupos da 2ª série C. Em seguida, expliquei os passos para a decodificação da mensagem que seria inicialmente encontrar a matriz inversa da matriz chave, e posteriormente a multiplicação da matriz inversa pela matriz mensagem codificada.

Figura 4 – Alunos codificando a mensagem

Fonte: Próprio autor

Figura 5 – Alunos decodificando as mensagens

Fonte: Próprio autor

Para realização dos cálculos foi permitido o uso da função calculadora no celular pelos estudantes. Vale lembrar que, durante a realização da atividade os grupos solicitaram auxílio para encontrar a matriz inversa, sendo assim os mesmos foram auxiliados por mim e pelo docente responsável pelas turmas.

Após todos os grupos terem concluído a decodificação da mensagem na 2ª série A "A leitura engrandece a alma", informei aos alunos que a mensagem dava dica sobre o local onde o tesouro estava escondido e pedi que um membro de cada grupo me acompanhasse para a busca. Os estudantes não tiveram duvidas quanto a localização e logo indicaram a sala de leitura como o local do esconderijo.

Na sequência a próxima turma a decodificar a mensagem foi a 2ª série B encontrando o tesouro na sala de informática, através da dica presente na mensagem "Informática o hardware da vida". E por fim, a 2ª série C localizou o tesouro no refeitório por meio da mensagem "O melhor tempero da comida é a fome".

Figura 6 – O encontro do tesouro pelos alunos

Fonte: Próprio autor

Figura 7 – O encontro do tesouro pelos alunos 2

Fonte: Próprio autor

5 - CONCLUSÃO

Através desta prática pude conhecer o prazer de ensinar matemática, pois a atividade foi empolgante, todos os alunos ficaram envolvidos e se empenharem na codificação e decodificação das mensagens, afim de encontrarem o tesouro. Foi perceptível a felicidade dos estudantes no momento em que cada grupo encontrava a mensagem. Fiquei emocionada quando o docente da sala, após pedir a atenção dos alunos, mostrou a eles a comparação da emoção que estavam sentindo naquele momento e a emoção que os criptonalistas sentiram ao decodificar mensagens e decifrar as máquinas e num caso específico antecipar o final de uma guerra.

Sem dúvidas, aprendi a importância de preparar aulas que estimulem os alunos e despertem nestes o interesse, pois através do envolvimento dos estudantes na atividade é que se obtém o sucesso na aprendizagem.

6 – REFERÊNCIAS

ARINOS, Edgard José dos Santos. Criptografia: Aplicações no Ensino Fundamental e Médio. Campo Grande, 2014. Disponível em: file:///C:/Users/User/Downloads/2012_01586_EDGARD_JOSE_DOS_SANTOS_ARINOS.pdf

CALLIOLI, Carlos A. e outros. Álgebra linear e aplicações, 6ª edição reformulada. Disponível em: file:///C:/Users/User/Downloads/Álgebra%20Linear%20e%20Aplicações%20-%20Carlos%20A.%20Callioli%20(1).pdf

MARQUES, Thiago Valentim. Criptografia: abordagem histórica, protocolo Diffie – Hellmane aplicações em sala de aula. João Pessoa – PB, 2013. Disponível em: http://tede.biblioteca.ufpb.br/bitstream/tede/7545/5/arquivototal.pdf

NASCIMENTO, Desirée Bueno. Proposta de uma arquitetura de referência para o algoritmo Keccak. Marília, 2011. Disponível em: http://aberto.univem.edu.br/bitstream/handle/11077/370/Proposta%20de%20uma%20Arquitetura%20de%20Referência%20para%20o%20Algoritmo%20Keccak.pdf?sequence=1

PAES, Wilhelm dos Santos. Criptografia em Blocos: Um enfoque em sua aplicação no ensino de matrizes. Dourados, 2014. Disponível em: http://200.129.209.183/arquivos/arquivos/78/MESTRADO-MATEMATICA/CRIPTOGRAFIA%20EM%20BLOCOS%20UM%20ENFOQUE%20EM%20SUA%20Wilhelm%20Dos%20Santos%20Paes.pdf

TKOTZ, Viktoria. O que é criptoanálise. Disponível em http://www.numaboa.com.br/criptografia/criptoanalise/307-Criptoanalise, Acessado em 02/05/2016.

TKOTZ, Viktoria. Substituições monoalfabéticas. Disponível em: http://www.numaboa.com.br/criptografia. Acessado em 02/05/2016.