

Criptografia como ferramenta no ensino da matemática

Cintia K. Rosseto

Suetônio de A. Meira

Resumo

O presente trabalho trata a Criptografia como ferramenta de ensino nas aulas de Matemática, tendo em vista que o ensino da matemática está cada vez mais comprometido, principalmente por conta do desinteresse dos alunos e da grande defasagem com a qual chegam ao Ensino Fundamental II. Diante disso, propomos a utilização de temas que tragam significado à aprendizagem e cativem o estudante. A criptografia pode ser abordada em vários conteúdos dos Ensinos Fundamental e Médio, como funções e matrizes, assuntos abordados no presente trabalho. Pretendemos, com a utilização da Criptografia no ensino dos conteúdos matemáticos, proporcionar sentido ao conteúdo estudado, de forma que a aprendizagem torne-se significativa para o aluno. Apresentaremos alguns modelos de atividades que abordam o tema criptografia e poderão ser desenvolvidas durante o ensino de funções, no 9º ano do E.F. e 1º ano do E.M., e, no ensino de matrizes, no 2º ano do E.M.

Palavras-chave: Criptografia; Funções; Aprendizagem.

Abstract

The present work treats Cryptography as a teaching tool in Mathematics classes, considering that the teaching of mathematics is increasingly compromised, mainly due to the lack of interest of the students and the large gap with which they arrive in Elementary School II. In view of this, we propose the use of themes that bring meaning to learning and captivate the student. The cryptography can be approached in several contents of Elementary and High School, like functions and matrices, subjects approached in the present work. We intend, with the use of Cryptography in the teaching of mathematical contents, to provide meaning to the content studied so that learning becomes meaningful for the student. We will present some models of activities that address the topic of cryptography and can be developed during the classes of functions, in the 9th year of E.S. and 1st year of H.S. and in the classes of matrices, in the 2nd year of H.S.

Keywords: Cryptography; functions; learning.

1. Introdução

A criptografia está presente em diversas situações do nosso cotidiano. Com o advento da era digital, tudo ao nosso redor passou a utilizar algum tipo de código para proteção, sejam os códigos de barras utilizados em supermercados até troca de mensagens no celular.

A palavra criptografia tem origem grega, *kryptos* significa oculto e *graphos*, escrever. É a ciência que estuda maneiras de esconder o significado da mensagem, de modo que somente quem possui a chave consegue ter acesso ao seu conteúdo.

Os professores de matemática possuem papel substancial na melhoria dos dados referentes à qualidade no ensino dessa disciplina, dando aos alunos condições para que, vista muitas vezes com certo repúdio, torne-se atrativa. Nesse sentido, esse trabalho tem sua contribuição na tentativa de melhorar a relação entre os alunos e a matemática, partindo de conceitos aplicados dentro da temática da criptografia.

No ensino da matemática, a inserção do estudo da criptografia torna-se uma ferramenta de suma importância pois, além de um assunto interessante, é muito abrangente, uma vez que envolve diversos conteúdos tratados no ensino fundamental e médio, servindo como meio de instigar o aluno e tornar as aulas atrativas e significativas.

“A falta de aplicações para os temas estudados em classe é o defeito mais gritante do ensino da Matemática em todas as séries escolares.” (Lima, Elon Lages, 2007, pag. 144)

Um dos desafios encontrados pelos professores de matemática é fazer com que os alunos não só aprendam os conteúdos, mas se interessem em aprendê-los. Como forma de atenuar os obstáculos encontrados no ensino-aprendizagem em matemática, o presente trabalho visa a proposta de atividades utilizando a temática da criptografia. Para tanto, foram abordados conteúdos como funções, aplicadas entre os alunos do 9º ano do Ensino Fundamental, da Escola Municipal Profa. Soledade Domingues Iglêsias, em Lucélia-SP.

Essas aprendizagens só serão possíveis na medida em que o professor proporcionar um ambiente de trabalho que estimule o aluno a criar, comparar, discutir, rever, perguntar e ampliar ideias. (PCN, 1997, pag. 41)

2. Material e Métodos

(...) o ensino da Matemática prestará sua contribuição à medida que forem exploradas metodologias que priorizem a criação de estratégias, a comprovação, a justificativa, a argumentação, o espírito crítico, e favoreçam a criatividade, o trabalho coletivo, a iniciativa pessoal e a autonomia advinda do desenvolvimento da confiança na própria capacidade de conhecer e enfrentar desafios. (PCN, 1997, pag. 31)

O padrão de desenvolvimento do ensino e aprendizagem da Matemática deve ser a abordagem de assuntos que despertem a curiosidade e que desencadeiem um processo que permita a construção de novos conhecimentos. O tema Criptografia pode ser utilizado como gerador de atividades didáticas que permitem aprofundar, fixar, revisar e exercitar os conteúdos matemáticos desenvolvidos nos ensinos Fundamental e Médio.

Apresentamos algumas atividades que abordam Criptografia e conteúdos estudados nas aulas de Matemática. Tais atividades devem ser realizadas em grupo, com orientação prévia do professor.

Seguem modelos de atividades:

- Cifra de Substituição

Um dos primeiros sistemas de criptografia conhecido foi elaborado pelo general Júlio César. O sistema monoalfabético, conhecido como Cifra de César, consistia em substituir cada letra do alfabeto seguindo um padrão bem determinado. Acredita-se que Júlio César substituía cada letra, pela terceira letra que se segue no alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Assim, por exemplo, codificando a mensagem CRIPTOGRAFIA, temos FULSWRJUDILD.

Usando a Cifra de César podemos desenvolver atividades que podem ser aplicadas na introdução do estudo das funções.

O mesmo princípio pode ser utilizado deslocando-se diferentes quantidades de casa (chave), criando assim 26 possibilidades de substituições. Para facilitar o desenvolvimento das atividades, propomos a utilização dos discos giratórios, permitindo que os alunos criem e troquem mensagens criptografadas com os demais grupos.

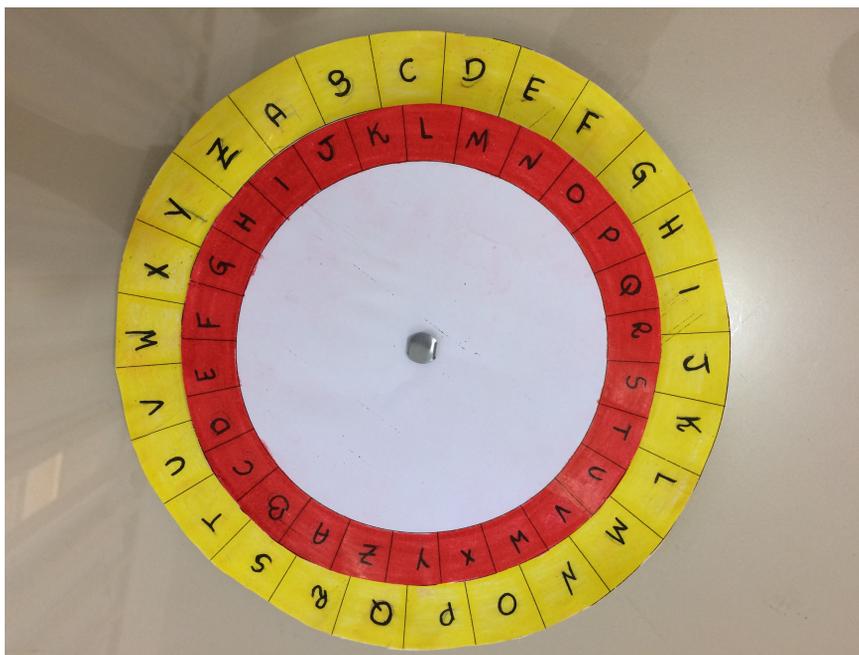


Figura 1: Disco giratório.

• Criptografia e Funções

O método de codificação deve ser perfeitamente eficaz, ou seja, o receptor deve ser capaz de transformar a informação codificada na informação original, sem ambiguidade ou falta de informação. Para isso, algumas propriedades devem ser seguidas nessas situações:

- i. ao codificar duas informações distintas, elas não podem ser transformadas em uma mesma informação codificada, pois o receptor teria dúvidas ao codificá-la;
- ii. uma informação, ao ser codificada, não pode produzir duas informações diferentes;
- iii. toda informação deve ter uma forma codificada, ou seja, toda e qualquer informação deve ser possível de ser transmitida, evitando informações incompletas.

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

Para que ocorra a codificação, cada informação deve ser transformada em uma única informação codificada e deve aceitar o processo inverso; portanto, devemos encontrar uma transformação bijetiva f . Como f é inversível, podemos garantir a revelação das informações.

Usaremos a função afim $f(x) = ax + b$. Essa função é sempre bijetiva sobre sua imagem e, por isso, admite inversa sobre sua imagem.

O método consiste em pegar uma informação e convertê-la em números através de uma função bijetiva e, pela aplicação de sua inversa, transformar esses números novamente na informação original.

Primeiramente, vamos associar cada letra do alfabeto a um número, como na tabela anterior.

Agora, escolhemos uma função $f(x)$ que receberá o valor da letra que queremos transmitir e gerar outro valor através de $f(x)$. Suponhamos que f seja a função $f(x) + 3x + 2$, que é chamada de função cifradora.

Escolhemos a palavra MENSAGEM que, ao passar pela função cifradora, será transformada na sequência de números 67 43 70 85 31 39 43 67. Esta é a mensagem que o receptor receberá.

$M \rightarrow 23$	$f(23) = 3 \times 23 - 2 = 67$
$E \rightarrow 15$	$f(15) = 3 \times 15 - 2 = 43$
$N \rightarrow 24$	$f(24) = 3 \times 24 - 2 = 70$
$S \rightarrow 29$	$f(29) = 3 \times 29 - 2 = 85$
$A \rightarrow 11$	$f(11) = 3 \times 11 - 2 = 31$
$G \rightarrow 17$	$f(17) = 3 \times 17 - 2 = 49$
$E \rightarrow 15$	$f(15) = 3 \times 15 - 2 = 43$
$M \rightarrow 23$	$f(23) = 3 \times 23 - 2 = 67$

O receptor, ao receber a mensagem codificada, realizará a operação inversa, que nesse caso é $f^{-1}(x) = \frac{x+2}{3}$, recompondo a mensagem original.

$f^{-1}(67) = \frac{67+2}{3} = 23$	$23 \rightarrow M$
$f^{-1}(43) = \frac{43+2}{3} = 15$	$15 \rightarrow E$
$f^{-1}(70) = \frac{70+2}{3} = 24$	$24 \rightarrow N$
$f^{-1}(85) = \frac{85+2}{3} = 29$	$29 \rightarrow S$
$f^{-1}(31) = \frac{31+2}{3} = 11$	$11 \rightarrow A$
$f^{-1}(49) = \frac{49+2}{3} = 17$	$17 \rightarrow G$
$f^{-1}(43) = \frac{43+2}{3} = 15$	$15 \rightarrow E$
$f^{-1}(67) = \frac{67+2}{3} = 23$	$23 \rightarrow M$

Quanto mais complexo for o código, mais difícil a mensagem fica para ser decifrada.

- Cifras de Hill

As cifras de Hill, baseadas em transformações matriciais utilizando um sistema poligráfico, foram inventadas por Lester S. Hill em 1929.

Atribuiremos um número a cada letra do alfabeto da seguinte forma:

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

Codificaremos a frase VAMOS CODIFICAR e para isso devemos transformar pares sucessivos de texto em texto cifrado. Devemos escolher uma matriz quadrada; para facilitar escolheremos uma matriz 2×2 .

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Agruparemos letras sucessivas de texto em pares, substituindo cada letra por seu valor numérico. Caso tenha um número ímpar de letras, acrescentaremos uma letra fictícia para completar o último par.

V	A	M	O	S	C	O	D	I	F	I	C	A	R
22	1	13	15	19	3	15	4	9	6	9	3	1	18

Converteremos cada par sucessivo p_1 e p_2 de letras de texto em um vetor-coluna.

$$p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

e formaremos o produto Ap (vetor cifrado).

A matriz cifradora deve ser invertível módulo 26.

$$\text{Usaremos a matriz } \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

Para cifrar o par VA efetuaremos o produto matricial

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 22 \\ 1 \end{bmatrix} = \begin{bmatrix} 116 \\ 47 \end{bmatrix}$$

Sempre que ocorrer um inteiro maior do que 25, ele será substituído pelo resto da divisão desse inteiro por 26.

$$\text{Assim, } \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 22 \\ 1 \end{bmatrix} = \begin{bmatrix} 116 \\ 47 \end{bmatrix} \equiv \begin{bmatrix} 12 \\ 21 \end{bmatrix} \pmod{26}$$

que fornecerá o texto cifrado LU.

Os cálculos para os demais vetores cifrados são

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} 155 \\ 71 \end{bmatrix} \equiv \begin{bmatrix} 25 \\ 19 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 3 \end{bmatrix} = \begin{bmatrix} 113 \\ 47 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 21 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 15 \\ 4 \end{bmatrix} = \begin{bmatrix} 99 \\ 42 \end{bmatrix} \equiv \begin{bmatrix} 21 \\ 16 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 6 \end{bmatrix} = \begin{bmatrix} 81 \\ 36 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 10 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 3 \end{bmatrix} = \begin{bmatrix} 63 \\ 27 \end{bmatrix} \equiv \begin{bmatrix} 11 \\ 1 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} 113 \\ 56 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 4 \end{bmatrix} \pmod{26}$$

A mensagem transmitida será LUYSIUUPCJKAID.

Para decifrar devemos multiplicar cada vetor cifrado pelo inverso de A , que será obtido da seguinte forma:

$$A^{-1} = (a_{11} \cdot a_{22} - a_{12} \cdot a_{21})^{-1} \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \pmod{26}$$

onde $(a_{11} \cdot a_{22} - a_{12} \cdot a_{21})^{-1}$ é o recíproco do resíduo de $(a_{11} \cdot a_{22} - a_{12} \cdot a_{21}) \pmod{26}$.

Para auxiliar os cálculos abaixo, forneceremos a tabela de recíprocos módulo 26.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Assim,

$$\det A = \begin{vmatrix} 5 & 6 \\ 2 & 3 \end{vmatrix} = 15 - 12 = 3$$

$$A^{-1} = 3^{-1} \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = 9 \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix} \equiv \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \pmod{26}$$

Os cálculos para decifrar os vetores cifrados são

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 12 \\ 21 \end{bmatrix} = \begin{bmatrix} 516 \\ 495 \end{bmatrix} \equiv \begin{bmatrix} 22 \\ 1 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 25 \\ 19 \end{bmatrix} = \begin{bmatrix} 481 \\ 561 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 15 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 9 \\ 21 \end{bmatrix} = \begin{bmatrix} 513 \\ 471 \end{bmatrix} \equiv \begin{bmatrix} 19 \\ 3 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 21 \\ 16 \end{bmatrix} = \begin{bmatrix} 405 \\ 472 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 4 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 3 \\ 10 \end{bmatrix} = \begin{bmatrix} 243 \\ 214 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 6 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 11 \\ 1 \end{bmatrix} = \begin{bmatrix} 35 \\ 107 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 3 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \begin{bmatrix} 9 \\ 4 \end{bmatrix} = \begin{bmatrix} 105 \\ 148 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 18 \end{bmatrix} \pmod{26}$$

Os equivalentes alfabéticos desses vetores são VA MO SC OD IF IC AR que fornecem a mensagem "vamos codificar".

- Cifra de Vigenère

CIFRA DE VIGNÈRE

	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

Figura 2: Cifra de Vignère.

A cifra de Vignère é uma versão simplificada da cifra de substituição polialfabética, inventada em 1465, por Leon Battista Alberti, conhecido como pai da criptologia ocidental. Recebeu esse nome em homenagem a Blaise de Vignère, diplomata e criptógrafo francês, mas o primeiro registro foi descrito por Giovan Batista Belaso em *La cifra del Signore Giovan Batista Belaso*, de 1553.

A cifra de Vignère usa não apenas um, e sim 26 alfabetos cifrados distintos para criar a mensagem cifrada. Além da tabela, Vignère inseriu palavras-chave utilizadas na codificação e na decodificação da mensagem.

Como exemplo, considere que a palavra-chave seja GATO e que a mensagem seja VAMOS ATACAR. Repetiremos a chave até acabarem as letras da mensagem, da seguinte forma:

Chave	G	A	T	O	G	A	T	O	G	A	T
Mensagem	V	A	M	O	S	A	T	A	C	A	R

Para codificarmos a mensagem procuraremos na Figura 2 a interseção da chave (linha) com a mensagem (coluna). Assim,

Chave	G	A	T	O	G	A	T	O	G	A	T
Mensagem	V	A	M	O	S	A	T	A	C	A	R
Codificado	B	A	E	C	Y	A	M	O	I	A	R

3. Resultados e Discussão

O significado da atividade matemática para o aluno também resulta das conexões que ele estabelece entre ela e as demais disciplinas, entre ela e seu cotidiano, e das conexões que ele percebe entre os diferentes temas matemáticos. (PCN, 1997, pag. 38)

A criptografia como ferramenta de ensino é de grande valia, conseguimos relacionar Matemática e História, mostramos aplicações no dia a dia, ressaltamos a importância da Matemática, e, principalmente, cativamos os alunos.

Os alunos envolvidos nas atividades demonstraram mais entusiasmo durante as aulas, maior dedicação e uma melhora significativa no rendimento escolar. A repercussão das atividades resultou na criação da Oficina de Criptografia, que permitiu a participação de alunos dos demais anos.

As atividades foram executadas no segundo e terceiro bimestres. Nesse período, percebemos uma melhora no desempenho escolar dos estudantes, como mostra a tabela a seguir

	1º Bimestre	2º Bimestre	3º Bimestre
9º ano B	6,4	7,2	7,3
9º ano E	5,6	6,1	6,8

4. Conclusão

Partindo dos resultados preliminares, podemos concluir que os alunos envolvidos obtiveram melhor rendimento nas aulas, além do ganho cultural.

Usando a criptografia como ferramenta no ensino, atribuímos significado ao conceito estudado, de forma que o aluno sinta-se motivado a aprendê-lo. Assim, ressaltamos a importância de inserir o uso de assuntos ligados à realidade do aluno, que estimulem o empenho dos mesmos nas aulas, contribuindo de forma significativa para sua aprendizagem.

Referências

- [1] BRASIL, Secretaria da Educação Fundamental. *Parâmetros Curriculares Nacionais: Matemática*. MEC-SEF. 1997.

- [2] COUTINHO, Severino Collier. *Números Inteiros e Criptografia RSA* 1^a ed. Rio de Janeiro. Impa. 2014.
- [3] HEFEZ, Abramo. *Aritmética*. Coleção Profmat. 1^a ed. Rio de Janeiro. SBM. 2014.
- [4] LIMA, Elon Lages; *et al.* *A Matemática do Ensino Médio*. Volume 1. 10^a ed. Rio de Janeiro. SBM. 2010.
- [5] LIMA, Elon Lages. *Matemática e Ensino*. 3^a ed. Rio de Janeiro. SBM. 2007.
- [6] SINGH, Simon. *O Livro dos Códigos*. trad. Jorge Calife. 4^a ed. Rio de Janeiro. Record. 2004.

Cintia K. Rosseto
Universidade Estadual Paulista "Julio de Mesquita Filho" - Unesp
<cintia.kohori@gmail.com>

Suetônio de A. Meira
Universidade Estadual Paulista "Julio de Mesquita Filho" -Unesp
<toni.meira@gmail.com>

Recebido: 27/12/2020
Publicado: 11/03/2020