



## CRIOGRAFIA E O ENSINO DE FUNÇÃO AFIM E SUA INVERSA

Silvana Leal da Silva<sup>1</sup>

Karina França Bragança<sup>2</sup>

Ramon Chagas Santos<sup>3</sup>

Alex Cabral Barbosa<sup>4</sup>

### Educação Matemática no Ensino Médio

**Resumo:** Este trabalho foi desenvolvido como parte de um Trabalho de Conclusão de Curso da Licenciatura em Matemática do Instituto Federal Fluminense e tem como objetivo apresentar a Criptografia como ferramenta para tornar o ensino e aprendizagem de função afim e de sua inversa significativos. Esta pesquisa foi motivada pelo desejo de trabalhar um tema atual, dinâmico e presente no cotidiano dos educandos. A Criptografia, além de ser um tema presente na atualidade, apoia-se na matemática para assegurar o sigilo necessário na comunicação. Para tanto, o trabalho está voltado para alunos que já tenham estudado função afim e sua inversa, pois o intuito não é ensinar o conteúdo e sim trazer significado por meio da Criptografia. Essa proposta baseia-se na Teoria da Aprendizagem Significativa de Ausubel, cuja ideia central, segundo Moreira e Masini (2006), é a de que o fator mais importante da aprendizagem é aquilo que o aprendiz já sabe. Foi aplicada uma proposta pedagógica para alunos do segundo período de Licenciatura em Matemática, onde constatou-se que o fato de trabalhar com um tema potencialmente significativo e atual, motiva e contribui para dar significado aos conteúdos anteriormente trabalhados.

**Palavras Chaves:** Criptografia. Ensino Médio. Matemática.

### 1. INTRODUÇÃO

Optou-se por trabalhar Criptografia por ser um tema presente na atualidade (redes sociais, transações bancárias, compras on-line, entre outros) e se apoiar na matemática para assegurar o sigilo necessário na comunicação.

A importância de buscar-se métodos dinâmicos e temas atuais no processo de ensino e aprendizagem é mencionada nos Parâmetros Curriculares Nacionais do Ensino Médio – PCNEM (BRASIL, 2002). Este documento destaca a necessidade da educação se voltar para o desenvolvimento das capacidades de comunicação, de resolver problemas, aperfeiçoar conhecimentos e valores, visto que a sociedade está integrada a uma rede de informação crescentemente globalizada (BRASIL, 2002).

Mais especificamente, a função da Matemática segundo os PCNEM (BRASIL, 2002) é, e necessita ser, mais do que memorizar resultados oriundos dessa ciência.

---

<sup>1</sup> Licencianda em Matemática. IFFluminense. silva.sleal@gmail.com

<sup>2</sup> Licencianda em Matemática. IFFluminense. Karinabraganca14@gmail.com

<sup>3</sup> Licenciando em Matemática. IFFluminense. ramonchagassantos@hotmail.com

<sup>4</sup> Mestre em Pesquisa Operacional e Inteligência Computacional. IFFluminense. alex.barbosa@iff.edu.br

A obtenção do conhecimento matemático, precisa estar vinculada ao domínio de um saber fazer Matemática e de um saber pensar matemático (BRASIL, 2002).

Além disso, destaca-se a importância da contextualização e interdisciplinaridade, ou seja, permitir conexões entre diversos conceitos matemáticos e aplicações dentro ou fora da Matemática, conforme afirmado pelos PCNEM (BRASIL, 2002).

Nesse sentido, Pereira, V. (2012) considera a Criptografia uma temática com potencial didático para contextualização de conteúdos matemáticos. Este tema apresenta material útil para a compreensão de importantes conceitos matemáticos, podendo tornar as aulas de Matemática dinâmicas e motivadoras (PEREIRA, V., 2012).

Acerca do tema Criptografia, Pereira, N. (2015) afirma que:

Muitos conceitos matemáticos utilizados em Criptografia fazem parte da grade curricular do Ensino de Matemática. Dessa forma, associar os conceitos a uma aplicação tão corrente nos dias de hoje, torna a aprendizagem mais significativa (PEREIRA, N., 2015, p.6).

Alguns desses conceitos matemáticos utilizados na Criptografia, de acordo com Santos (2013) e Borges (2008) são os de funções, matrizes, análise combinatória, teoria dos números e geometria analítica.

Dentre esses conceitos, optou-se por desenvolver neste trabalho o tema funções e, mais especificamente, função afim e sua inversa, primeiro porque de acordo com os PCNEM (BRASIL, 2002), o ensino isolado deste tema não permite a exploração do caráter integrador que este possui, e segundo, pelo fato da função afim ser invertível. Esta característica é a garantia do processo de codificação de mensagens ser reversível e suas informações poderem ser reveladas pelos receptores (TAMAROZZI, 2001).

Esse trabalho está fundamentado na Teoria da Aprendizagem Significativa de Ausubel, cuja ideia central, segundo Moreira e Masini (2006), é a de que o fator mais importante da aprendizagem é aquilo que o aprendiz já sabe. Nessa teoria, a aprendizagem ocorre quando a nova informação interage com uma estrutura de conhecimento específica, a qual Ausubel chama de “subsunção”, existente na estrutura cognitiva de quem aprende (MOREIRA E MASINI, 2006).

Nessa interação,

conceitos mais relevantes e inclusivos interagem com o novo material servindo de ancoradouro, incorporando-o e assimilando-o, porém, ao mesmo tempo, modificando-se em função dessa ancoragem (MOREIRA, 2006).

Para que a aprendizagem seja significativa, segundo Moreira (2006), o novo material deve ser potencialmente significativo, ou seja, deve ser “logicamente significativo” ou ter “significado lógico” e estar relacionado com conceitos subsunções presentes na estrutura cognitiva do indivíduo; e o aprendiz deve estar disposto a aprender.

### **1.1 Aspectos Relevantes da História da Criptografia**

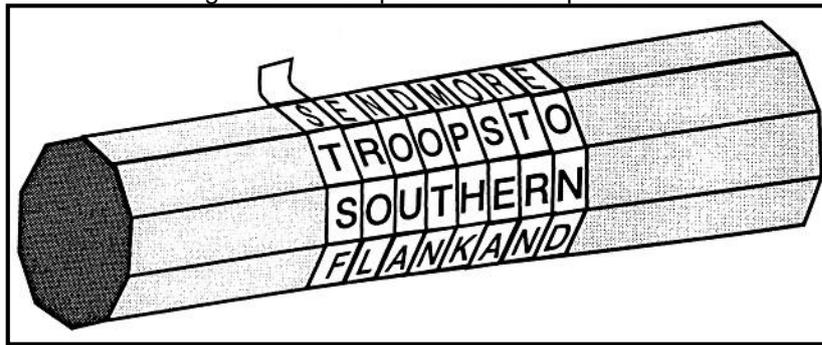
Segundo Tamarozzi (2001), Criptografia é uma palavra que vem do grego *kryptós*, de “oculto” e *gráphein* de “escrita”. A Criptografia utiliza métodos para transformar uma mensagem em um código, por meio de recursos matemáticos, de modo que apenas o seu destinatário legítimo consiga interpretá-lo.

Toda parte histórica, apresentada nessa subseção, baseia-se na obra “O livro dos códigos: A ciência do sigilo – do antigo Egito à criptografia quântica”, de Simon Singh (2001).

Durante anos, a necessidade de uma comunicação eficiente entre reis, rainhas e generais motivou a criação de mecanismos capazes de assegurar que informações sigilosas não fossem interceptadas. Um desses mecanismos de comunicação secreta é a Esteganografia que consiste em esconder a mensagem. Porém, esse mecanismo oferece pouca segurança, contribuindo assim para o desenvolvimento da Criptografia.

Um aparelho utilizado para criptografar mensagens é o Citale Espartano, composto por um bastão de madeira no qual é enrolada uma tira de couro contendo uma mensagem que desenrolada apresenta uma sequência aleatória de letras (Figura 1). A mensagem só será revelada quando enrolada em torno de um outro citale de mesmo diâmetro.

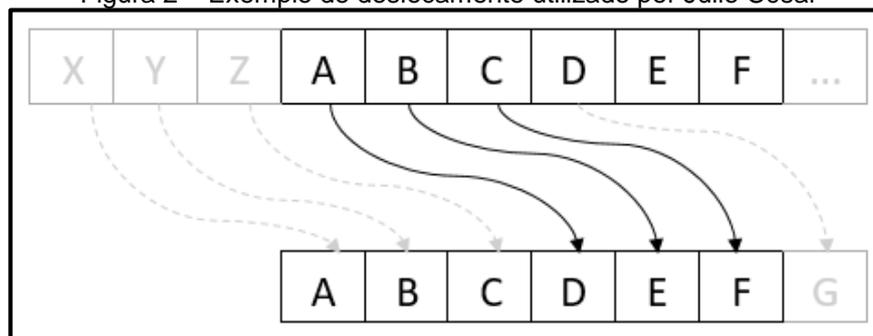
Figura 1 – Exemplo de Citale Espartano



Fonte: Singh (2001, p. 24).

Outro exemplo de Criptografia é a Cifra de César que consiste em deslocar o alfabeto em uma determinada quantidade de casas à frente (Figura 2). Essa especificação é conhecida como chave, que define o alfabeto cifrado exato que será usado na codificação.

Figura 2 – Exemplo de deslocamento utilizado por Júlio César

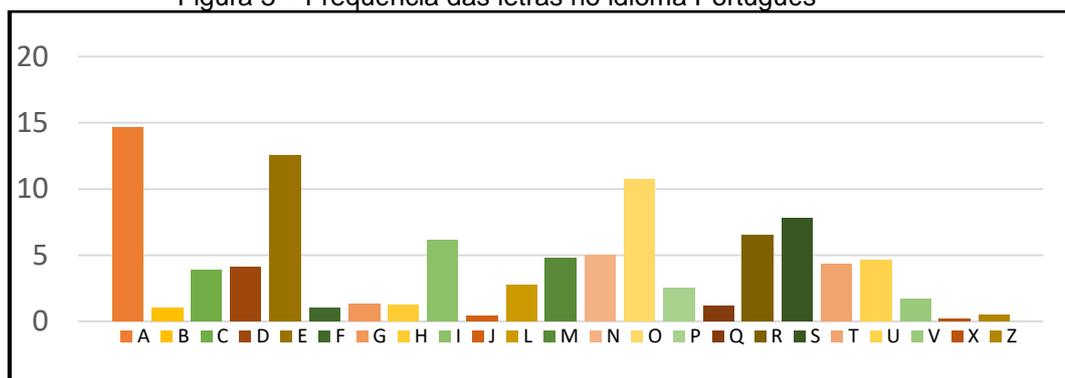


Fonte: Elaboração própria.

Muitos estudiosos achavam que esse tipo de cifra era inquebrável devido ao grande número de chaves envolvidas, contudo, surge a Criptoanálise, ciência que possibilita decifrar uma mensagem sem o conhecimento da chave.

A principal ferramenta da Criptoanálise é a análise de frequência. Essa técnica possibilita revelar o conteúdo de uma mensagem criptografada, analisando-se a frequência dos caracteres no texto cifrado de acordo com o idioma utilizado (Figura 3).

Figura 3 – Frequência das letras no idioma Português



Fonte: Elaboração própria.

Os processos que até então eram dados como seguros foram fragilizados, incitando a criação de cifras mais fortes, como a cifra de Vigenère, que consiste em uma tabela formada por 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior (Figura 4).

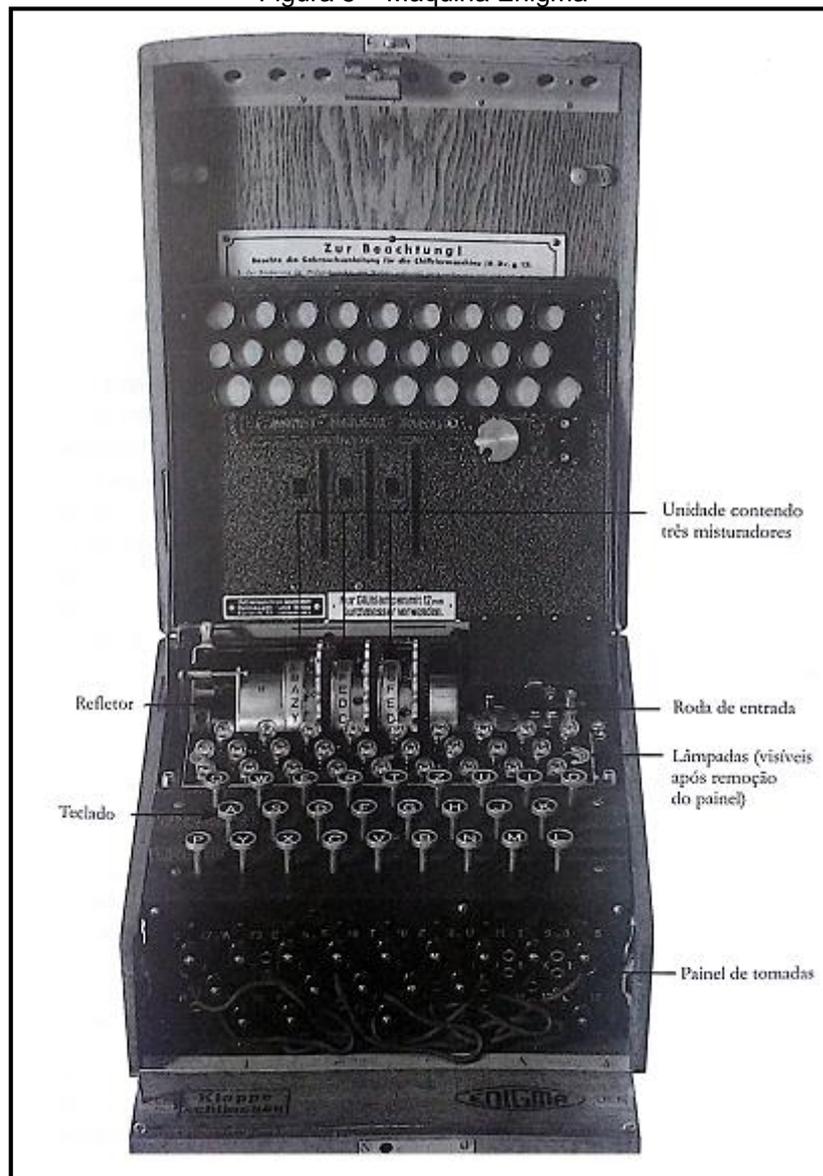
Figura 4 – Quadro de Vigenère

Alfabeto correto	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	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Fonte: Singh (2001, p.66).

Durante a Segunda Guerra Mundial, os alemães utilizaram a máquina Enigma (Figura 5), para enviar mensagens criptografadas aos seus exércitos.

Figura 5 – Máquina Enigma



Fonte: Singh (2001, p. 159).

A Inglaterra convocou especialistas para decifrarem a Enigma. Dentre eles, destaca-se Alan Turing, que criou as bombas de Turing e quebrou a cifra da Enigma.

Além das bombas de Turing, usadas para quebrar a cifra Enigma, os britânicos inventaram outro aparelho decifrador, o Colossus, para combater uma forma ainda mais poderosa de cifra, a cifra alemã Lorenz. Dos dois tipos de máquinas decifradoras, foi a Colossus que determinou o desenvolvimento da criptografia na segunda metade do século XX (SINGH, 2001, p.267).

Ao longo de sua história, a Criptografia foi prejudicada pela dificuldade na distribuição de chaves, pois antes da troca de mensagens era necessário o compartilhamento da chave a ser utilizada, o que muitas vezes era realizado por uma terceira parte, e isto enfraquecia a segurança.

Com intuito de solucionar este problema, o criptógrafo Whitfield Diffie e o professor Martin Hellman começaram a realizar estudos de modo a encontrar uma alternativa de transportar fisicamente as chaves ao longo de grandes distâncias em segurança. Mais tarde, Ralph Merkle se uniu a eles nessa pesquisa.

Eles criaram um modelo de caixa com dois cadeados que não funciona na vida real, mas contribuiu na busca da solução do problema da distribuição de chaves. Eles voltaram suas pesquisas para as funções matemáticas, que são operações que transformam um número em outro. Mais especificamente, eles buscavam funções fáceis de fazer e difíceis de desfazer, chamadas de funções de mão única com o intuito de solucionar este problema, mas foram outros três pesquisadores que conseguiram criar a cifra mais influente da Criptografia moderna, a cifra RSA.

A Criptografia de chave pública RSA acabou com o problema da distribuição de chaves dando uma clara vantagem aos criptógrafos.

Com isso, cientistas tentam construir um novo computador capaz de realizar cálculos em velocidade avançada, os computadores quânticos, contribuindo para a quebra da RSA.

Experiências anteriores mostraram que cifras consideradas inquebráveis sucumbiram ao ataque de criptoanalistas. Prevendo a chegada dos computadores quânticos, os criptógrafos trabalham em uma solução que coloque um fim na batalha entre criadores e quebradores de códigos. Com base na teoria quântica, busca-se um sistema de cifragem inquebrável, a criptografia quântica.

## **1.2 Criptografia na Atualidade**

“Com o advento da comunicação eletrônica, muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e uso seguro da Internet” (MALAGUTTI, 2015, p. 1).

Nos dias atuais, enviar e receber arquivos, navegar por redes sociais, trocar e-mails, realizar compras on-line, realizar transações bancárias, entre outras ações, têm se tornado cada vez mais comum na vida das pessoas, porém existe uma preocupação em relação à segurança desses recursos. A grande responsável para garantir que a segurança ocorra de forma eficiente é a Criptografia (PEREIRA, N., 2015).

Segundo Dantas (2016), a criptografia e a Matemática estão interligadas e fazem parte do dia a dia de qualquer indivíduo, inclusive dos estudantes, quando realizam alguma das ações citadas anteriormente.

A utilização da criptografia como ferramenta nas aulas de matemática possibilita que a aprendizagem tenha muito mais sentido e significado para os alunos, pois os saberes escolares estão relacionados ao seu cotidiano, contribuindo assim com o processo de ensino e aprendizagem. (DANTAS, 2016).

Um exemplo de abordagem desse tema no meio acadêmico, encontra-se nas apostilas (Figura 6) de “Criptografia” e “Atividades de Contagem a partir da Criptografia” do Programa de Iniciação Científica da Olimpíada Brasileira de Matemática das Escolas Públicas (PIC-OBMEP), que visa dar continuidade à formação matemática dos estudantes medalhistas da OBMEP. A Criptografia é utilizada como auxílio na exploração e aplicação de conceitos matemáticos, tais como números inteiros, aritmética modular e análise combinatória.

Figura 6 – Apostilas da OBMEP



Fonte: <http://www.obmep.org.br/apostilas.htm>

## 2. PROPOSTA PEDAGÓGICA

A presente proposta pedagógica tem como objetivo apresentar os aspectos relevantes da história da Criptografia por meio de vídeos, slides explicativos, apresentação oral e atividades, além de propor atividades onde a Criptografia interage com o conteúdo matemático Função Afim e sua inversa.

No primeiro momento é apresentado aspectos relevantes da evolução da Criptografia, tais como, definição de Criptografia e seu surgimento, Esteganografia, Citale Espartano, Cifra de César, Análise de Frequência, Cifra de Vigenère, Máquina

Enigma e a II Guerra Mundial, Popularização dos computadores e o problema da distribuição de chaves, Idealização da chave assimétrica, Cifra RSA, e a atualidade.

No segundo momento é realizado atividades que relacionam a Criptografia com o conteúdo de função afim e sua inversa, ocorrendo interação destes conceitos com intuito de trazer significado ao ensino e aprendizagem deste conteúdo matemático.

Na atividade 1 (Figura 7), os grupos deverão cifrar numericamente a mensagem utilizando o disco e determinar a função afim que representa a chave utilizada no processo.

Figura 7 – Atividade 1

Utilizando a palavra CODIGO:

a) Indique a sequência numérica associada;

C	O	D	I	G	O

b) Cifre usando a chave "avance quatro casas", e indique a nova sequência numérica;

c) Escreva a mensagem cifrada.

d) Como a chave cifradora poderia ser escrita em linguagem matemática?

Fonte: Elaboração própria.

Na atividade 2, cada grupo deverá cifrar uma mensagem utilizando a função afim dada como chave (Figura 8).

Figura 8 – Atividade 2

Cifre a palavra C R I P T O G R A F I A, utilizando a função cifradora  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  definida por  $f(x) = 3x + 1$ .

Fonte: Elaboração própria.

Na atividade 3, cada grupo deverá descobrir a mensagem cifrada, utilizando a função inversa da função afim dada (Figura 9).

Figura 9 – Atividade 3

A mensagem T M A C A M L Q C E S G S foi cifrada a partir da função cifradora  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  definida por  $f(x) = x - 2$ . Você seria capaz de descobrir a mensagem original?

Fonte: Elaboração própria.

Na atividade 4, (Figura 10) será necessário cifrar e decifrar mensagens (itens a e b) e, em seguida, resolver os demais itens utilizando o raciocínio lógico, além dos demais mecanismos apresentados.

Figura 10 – Atividade 4

(OBMEP, 2007 – Adaptada) Utilizando a chave “avance quatro casas”, a palavra PAI é cifrada como 20 – 5 – 13.

- a) Cifre OBMEP usando a chave “avance dezenove casas”.
- b) Usando a chave “avance 7 casas”, descubra qual palavra foi cifrada como 14 – 12 – 22 – 20 – 12 – 27 – 25 – 16 – 8.
- c) Bernardo cifrou uma palavra de 4 letras com a chave “avance dezenove casas”, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Bernardo colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele cifrou.
- d) Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?

Fonte: Elaboração própria.

### 3. APLICAÇÃO DA PROPOSTA PEDAGÓGICA

A proposta pedagógica foi aplicada para alunos do segundo período do curso de Licenciatura em Matemática, pois já haviam estudado função afim e sua inversa, com o intuito de verificar se o tema Criptografia contribui para tornar o ensino e aprendizagem de função afim e sua inversa significativos.

A priori, os alunos foram questionados sobre terem visto alguma aplicação de função inversa durante seu estudo, porém as respostas obtidas foram todas negativas.

A aplicação ocorreu em dois dias, com 12 participantes no primeiro dia e 10 no segundo. Porém, só foram validados os resultados de 7 participantes que estavam presentes em ambos encontros.

No primeiro dia após serem apresentados os aspectos relevantes da história da criptografia, foi possível perceber a empolgação e interação dos alunos com todo conteúdo apresentado, materiais construídos e vídeos apresentados sem demonstrar dificuldades.

Destacam-se alguns comentários pertinentes ao primeiro dia de aplicação:

Participante 1: “ O trabalho é muito interessante, diferente! As atividades são motivadoras e estimulam a participação.

Participante 2: “ Mostra bastante métodos que podemos aplicar no nosso dia-a-dia mostra que a matemática pode sim sair de dentro de sala de aula de uma maneira interessante. A credito que vai ser bastante proveitoso para alunos. ”

No segundo dia, os participantes resolveram as atividades de maneira investigativa, podendo contar com o auxílio dos autores do trabalho. Pôde-se perceber o bom desenvolvimento das atividades devido estarem familiarizados com o tema trabalhado.

Sobre o segundo dia, destaca-se o comentário do participante 3: “ As atividades propõe aos alunos uma forma lúdica e criativa para se trabalhar função afim e sua inversa, possibilitando sem dúvidas uma exelente participação dos alunos. As atividades propõem bons graus de desafios e que provavelmente será motivador e instigante para aqueles que participarem. “

#### **4. CONSIDERAÇÕES**

A Criptografia é um tema abrangente e atual, sua história é bem rica e interessante; e podemos concluir que é potencialmente significativo, sendo assim, uma das motivações para a realização deste trabalho. As atividades propostas são exemplos de recursos didáticos que o professor pode utilizar em sala de aula com os alunos, a fim de fixar, exercitar e revisar os conteúdos já estudados, possibilitando a alunos, futuros professores e professores um estudo acerca deste tema relacionado ao conteúdo de função afim e sua inversa, proporcionando significado à aprendizagem, e incentivando uma adequação a temáticas contemporâneas de uso diário. Além da matemática na criptografia, o professor tem a oportunidade de, em sala de aula, promover um debate social, sobre utilização de softwares e aplicativos com criptografia de ponta a ponta. Um debate de alta complexidade, pois a criptografia pode ser entendida por algumas pessoas, como uma violação de direitos de privacidade, enquanto para outras pessoas, como uma forma de proteção contra indivíduos que possam querer promover alguns tipos de danos à humanidade, como por exemplo, o terrorismo. Enfim, a criptografia está inserida em vários temas da atualidade, dando oportunidade ao professor, ao aluno, e ao leitor, entender melhor alguns aspectos da matemática estudada no ensino médio.

#### **REFERÊNCIAS**

BORGES, Fábio. Criptografia como Ferramenta para o Ensino de Matemática. In: Congresso Nacional de Matemática Aplicada e Computacional (CNMAC), 31., 2008, Belém. **Anais...** Belém: Sociedade Brasileira de Matemática Aplicada e Computacional, 2008. p. 822-828. Disponível em:

<[http://www.sbmac.org.br/eventos/cnmac/xxxi\\_cnmac/PDF/189.pdf](http://www.sbmac.org.br/eventos/cnmac/xxxi_cnmac/PDF/189.pdf)>. Acesso em: 26 dez. 2016.

BRASIL. Secretaria da Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais para o Ensino Médio**. Brasília: MEC, 2002.

DANTAS, Andréa de Araújo. **A Criptografia no Ensino Fundamental e Médio**. Monografia (Curso de Especialização em Ensino de Matemática para Ensino Médio) – Universidade Federal do Rio Grande do Norte, Caicó, 2016.

MALAGUTTI, Pedro. **Atividades de Contagem a partir da Criptografia**. Rio de Janeiro, IMPA, 2015.

MOREIRA, Marco Antonio. **A teoria da aprendizagem significativa e sua implementação em sala de aula**. Brasília: Editora Universidade de Brasília, 2006.

MOREIRA, Marco Antonio; MASINI, Elcie F. Salzano. **Aprendizagem significativa: a teoria de David Ausubel**. 2. ed. São Paulo: Centauro, 2006.

PEREIRA, Nádia Marques Ikeda. **Criptografia: uma nova proposta de ensino de matemática no ciclo básico**. 2015. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista Júlio de Mesquita Filho, Ilha Solteira, 2015. Disponível em: <<http://repositorio.unesp.br/bitstream/handle/11449/127733/000844677.pdf?sequence=1&isAllowed=y>>. Acesso em: 26 dez. 2016.

PEREIRA, Viviane da Silva Stellet. **Ensino de Funções: Uma Abordagem Contextualizada Sobre o Tratamento da Informação no Ensino Médio**. 2012. Dissertação (Mestrado em Educação Matemática) – Universidade Severino Sombra, Vassouras, 2012.

SANTOS, José Luiz dos. **A Arte de Cifrar, Criptografar, Esconder e Salvar como Fontes Motivadoras para Atividades de Matemática Básica**. 2013. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Matemática, Universidade Federal da Bahia, Salvador, 2013. Disponível em: <[http://bit.profmtat-sbm.org.br/xmlui/bitstream/handle/123456789/208/2011\\_00046\\_JOSE\\_LUIZ\\_DOS\\_SANTOS.pdf?sequence=1](http://bit.profmtat-sbm.org.br/xmlui/bitstream/handle/123456789/208/2011_00046_JOSE_LUIZ_DOS_SANTOS.pdf?sequence=1)>. Acesso em: 26 dez. 2016.

SINGH, Simon. **O livro dos códigos: A ciência do sigilo – do antigo Egito à criptografia quântica**. Tradução de Jorge Calife. Rio de Janeiro: Record, 2001.

TAMAROZZI, Antonio Carlos. Codificando e decifrando mensagens. **Revista do Professor de Matemática**, São Paulo: Sociedade Brasileira de Matemática, n. 45, p. 41-43, 2001.