LICENCIATURA EM MATEMÁTICA

CRIPTOGRAFIA: UMA FERRAMENTA PARA O ESTUDO DE FUNÇÃO AFIM E DE SUA INVERSA

SILVANA LEAL DA SILVA

RAMON CHAGAS SANTOS

KARINA FRANÇA BRAGANÇA

Campos dos Goytacazes – RJ

2017

SILVANA LEAL DA SILVA

RAMON CHAGAS SANTOS

KARINA FRANÇA BRAGANÇA

CRIPTOGRAFIA: UMA FERRAMENTA PARA O ESTUDO DE FUNÇÃO AFIM E DE SUA INVERSA

Monografia apresentada à Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia Fluminense *Campus* Campos Centro, como requisito parcial para conclusão do Curso de Licenciatura em Matemática.

Orientadora: Me. Lívia Azelman de Faria Abreu

Coorientador: Me. Alex Cabral Barbosa

Campos dos Goytacazes – RJ

2017

Biblioteca Anton Dakitsch
CIP - Catalogação na Publicação

S586c

Silva, Silvana Leal da
Criptografia: Uma ferramenta para o estudo de função afim e de sua inversa / Silvana Leal da Silva, Ramon Chagas Santos, Karina França Bragança - 2017.
178 f.: il. color.

Orientadora: Lívia Alzeman de Faria Abreu
Coorientador: Alex Cabral Barbosa

Trabalho de conclusão de curso (graduação) -- Instituto Federal de Educação, Ciência e Tecnologia Fluminense, Campus Campos Centro, Curso de Licenciatura em Matemática, Campos dos Goytacazes, RJ, 2017.
Referências: f. 99 a 102.

1. Criptografia. 2. Função Afim. 3. Função Inversa. 4. Contextualização. 5. Aprendizagem Significativa. I. Santos, Ramon Chagas. II. Bragança, Karina França. III. Abreu, Lívia Alzeman de Faria, orient. IV. Título.IV. Barbosa, Alex Cabral, coorient. V. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da Biblioteca Anton Dakitsch do IFF com os dados fornecidos pelo(a) autor(a).

SILVANA LEAL DA SILVA

RAMON CHAGAS SANTOS

KARINA FRANÇA BRAGANÇA

CRIPTOGRAFIA: UMA FERRAMENTA PARA O ESTUDO DE FUNÇÃO AFIM E DE SUA INVERSA

Monografia apresentada à Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia Fluminense *Campus* Campos Centro, como requisito parcial para conclusão do Curso de Licenciatura em Matemática.

Aprovada em 21 de setembro de 2017.

Banca Avaliadora:

Lívia Azelman de Faria Abreu

Prof.ª Lívia Azelman de Faria Abreu (orientadora)
Mestra em Matemática / PROFMAT – UENF
Instituto Federal de Educação, Ciência e Tecnologia Fluminense campus campos Centro

Alex Cabral Barbosa

Prof.º Alex Cabral Barbosa (coorientador)
Mestre em Pesquisa Operacional e Inteligência Computacional / UCAM
Instituto Federal de Educação, Ciência e Tecnologia Fluminense campus campos Centro

Gilmara T. Barcelos

Prof.ª Gilmara Teixeira Barcelos Peixoto
Doutora em Informática na Educação / UFRGS
Instituto Federal de Educação, Ciência e Tecnologia Fluminense campus campos Centro

Ana Paula Rangel de Andrade

Prof.ª Ana Paula Rangel de Andrade
Mestre em Planejamento Regional e Gestão da Cidade / UCAM
Instituto Federal de Educação, Ciência e Tecnologia Fluminense campus campos Centro

AGRADECIMENTOS

Gostaríamos de registrar nossos mais sinceros agradecimentos a todos que de alguma forma contribuíram para a realização e conclusão desta etapa tão fundamental para nossa formação.

Agradecemos a Deus, por iluminar nossos caminhos e nos dar forças para superar mesmo os mais difíceis obstáculos, permitindo que chegássemos até aqui.

Agradecemos a nossa orientadora Lívia Azelman de Faria Abreu, pela colaboração no desenvolvimento deste trabalho e pelo carinho e dedicação conosco. Agradecemos ao coorientador Alex Cabral Barbosa pela contribuição nesta nossa jornada.

Agradecemos também aos nossos familiares, colegas de classe e a todos que de alguma forma nos apoiaram até este momento. Em especial, as professoras Ana Paula Rangel de Andrade e Gilmara Teixeira Barcelos, que aceitaram participar da banca de avaliação deste trabalho.

Agradecemos aos participantes do teste exploratório e aos alunos da experimentação que cooperaram para obtenção dos resultados apresentados.

A todos o nosso muito obrigado.

Tudo é possível. O impossível apenas demora mais.

Dan Brown – Fortaleza Digital

RESUMO

A Criptografia é um tema dinâmico, atual e presente no cotidiano dos educandos. Além disso, apoia-se na Matemática para assegurar o sigilo na comunicação. A partir de pesquisas realizadas, pode-se perceber a relação deste tema com diversos conteúdos matemáticos. Sendo assim, esse trabalho monográfico tem como objetivo investigar as contribuições da Criptografia no processo de ensino e aprendizagem de função afim e sua inversa no Ensino Médio. Com o intuito de alcançar tal objetivo, elaborou-se uma sequência didática dividida em três momentos. No primeiro momento traçou-se o perfil dos alunos e diagnosticou-se seus conhecimentos sobre função afim e sua inversa. No segundo, foi apresentado o desenvolvimento da Criptografia. E por fim, fez-se a relação entre a Criptografia e a função afim e sua inversa. Os dados foram coletados por meio de diário de bordo, questionários e respostas das atividades. Essa pesquisa é do tipo intervenção pedagógica, tem caráter qualitativo e busca tornar a aprendizagem de função afim e sua inversa significativa, por meio da contextualização proporcionada pela Criptografia. Os resultados obtidos, mostram que a apresentação dessa relação, contribui para o processo de ensino e aprendizagem desses conteúdos, atribuindo significado ao seu estudo.

Palavras-chave: Criptografia. Função Afim. Função Inversa. Contextualização. Aprendizagem Significativa.

ABSTRACT

Cryptography is a dynamic theme, present and present in the daily life of learners. In addition, it relies on Mathematics to ensure confidentiality in communication. From the researches carried out, one can perceive the relation of this theme with several mathematical contents. Thus, this monographic work aims to investigate the contributions of Cryptography in the process of teaching and learning of related function and its inverse in High School. In order to achieve this goal, a didactic sequence was elaborated divided into three moments. In the first moment the profile of the students was traced and their knowledge about related function and its inverse was diagnosed. In the second, the development of Cryptography was presented. And finally, the relation between Cryptography and the related function and its inverse was made. The data were collected through logbook, questionnaires and responses of the activities. This research is pedagogical intervention type, has a qualitative character and seeks to make the learning of affine function and its inverse significant, through the contextualization provided by Cryptography. The results show that the presentation of this relation contributes to the teaching and learning process of these contents, assigning meaning to their study.

Key words: Cryptography. Related Function. Reverse Function. Contextualization. Meaningful Learning.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

Esta pesquisa foi motivada pelo desejo de trabalhar com um tema atual, dinâmico e presente no cotidiano dos educandos. Após sugestão de um dos autores deste projeto, inspirado na leitura do livro "Fortaleza Digital" de Dan Brown[1], optou-se pelo tema Criptografia. Pesquisas foram realizadas sobre o assunto e constatou-se que, além deste tema estar presente na atualidade (redes sociais, transações bancárias, compras *on-line*, entre outros), apoia-se na Matemática para assegurar o sigilo necessário na comunicação.

A importância de buscarem-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. 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).

De acordo com Pinheiro (2012), a contextualização é uma possibilidade de dinamizar o ensino, envolvendo os alunos com o conhecimento científico inserido no seu cotidiano, permitindo assim uma significação da aprendizagem. Segundo os PCNEM, "é possível generalizar a contextualização como recurso para tornar a aprendizagem significativa ao associá-la com experiências da vida cotidiana ou com os conhecimentos adquiridos espontaneamente" (BRASIL, 2000, p. 81).

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:

---

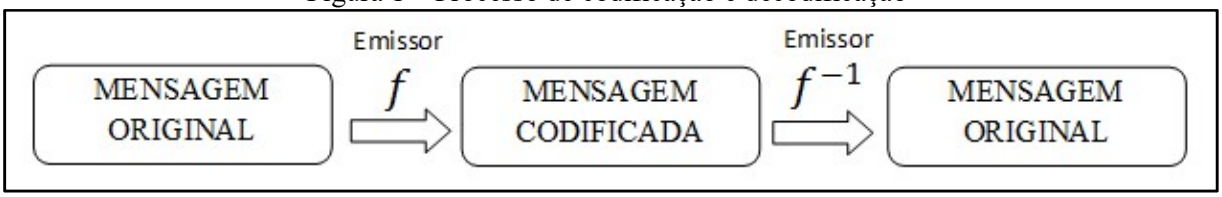
[1] BROWN, Dan. **Fortaleza Digital.** Tradução de Carlos Irineu da Costa. Rio de Janeiro: Sextante, 2005.

> 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, J. (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 ele possui, e segundo, pelo fato de a função afim ser invertível. Esta característica da invertibilidade, é a garantia de o processo de codificação de mensagens ser reversível e suas informações poderem ser reveladas pelos receptores (TAMAROZZI, 2001). O esquema a seguir ilustra este processo (Figura 1).

Figura 1 – Processo de codificação e decodificação



Fonte: Elaboração própria.

Uma pesquisa foi realizada em cinco dos seis livros didáticos[2] que fazem parte do Programa Nacional do Livro Didático – PNLD (BRASIL, 2014), com o intuito de analisar se os conceitos de função afim e sua inversa são expostos de forma contextualizada nesses livros. Observou-se que todos apresentam o conteúdo de função afim com clareza e aplicações, porém apenas quatro livros apresentam o conceito de função inversa da função afim. Destes, apenas um traz uma aplicação da função inversa, que utiliza a Criptografia.

Diante do que foi exposto, formulou-se a seguinte questão de pesquisa: Quais são as possíveis contribuições da Criptografia no ensino e aprendizagem de função afim e de sua inversa?

---

[2] DANTE, Luiz Roberto. **Matemática:** contexto & aplicações. 2. ed. São Paulo: Ática, 2013.
LEONARDO, Fabio Martins de (Ed.). **Conexões com a Matemática.** Organizadora Editora Moderna. 2. ed. São Paulo: Moderna, 2013.
PAIVA, Manoel. **Matemática:** Paiva. 2. ed. São Paulo: Moderna, 2013.
SMOLE, Kátia Stocco, DINIZ, Maria Ignez. **Matemática:** Ensino Médio. 8. ed. São Paulo: Saraiva, 2013.
SOUZA, Joamir Roberto de. **Novo Olhar:** Matemática. 2. ed. São Paulo: FTD, 2013.

Para responder tal questão, traçou-se o seguinte objetivo: investigar contribuições da Criptografia no processo de ensino e aprendizagem de função afim e de sua inversa para alunos do Ensino Médio. Para tanto, foram traçados os seguintes objetivos específicos:

- Promover um estudo sobre a Criptografia e suas aplicações na Matemática e no cotidiano;
- Diagnosticar os conhecimentos prévios dos alunos em relação aos conceitos de função afim e de sua inversa;
- Proporcionar conhecimento ao aluno sobre o tema, de forma dinâmica, por meio da apresentação de aspectos relevantes da evolução histórica da Criptografia;
- Possibilitar que a aprendizagem de função afim e de sua inversa seja significativa para o aluno utilizando a interdisciplinaridade existente entre Criptografia e Matemática.

O presente trabalho encontra-se estruturado em três capítulos, além desta Introdução e das Considerações Finais. O primeiro capítulo apresenta um breve histórico da Criptografia, sua presença no cotidiano, a aprendizagem significativa por meio da contextualização e resumos de trabalhos que abordam este mesmo tema. O segundo capítulo aborda os aspectos metodológicos, tais como metodologia de pesquisa adotada, instrumentos de coleta de dados, as etapas a serem desenvolvidas na pesquisa e o detalhamento da sequência didática. O terceiro capítulo apresenta o relato da aplicação do teste exploratório, com as modificações feitas na sequência didática a partir deste e o relato da experimentação, seguida da análise dos resultados obtidos. Por fim, são apresentadas as considerações finais e a resposta ao objetivo da pesquisa.

1. APORTE TEÓRICO

Neste capítulo, é apresentado o aporte teórico que embasou a elaboração deste trabalho monográfico. Subdividido em três seções, nas quais se discutem os aspectos relacionados a Criptografia, evolução histórica e atualidade, a aprendizagem significativa por meio da contextualização e estudos relacionados ao presente trabalho.

1.1 Criptografia

1.1.1 Aspectos Relevantes da História da Criptografia

Segundo Tamarozzi (2001), Criptografia é uma palavra que vem do grego *kryptós*, de "oculto" e *gráphein* de "escrita", e 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). Nesse sentido, para facilitar a leitura, não será repetida a referência a cada parágrafo.

Durante milhares de 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 por inimigos.

Um desses mecanismos de comunicação secreta é a esteganografia (do grego *steganos,* "coberto" e *graphein,* "escrita") que consiste em esconder a mensagem de diferentes maneiras, como por exemplo, raspando-se a cabeça do mensageiro, escrevendo a mensagem em seu couro cabeludo e o enviando ao destinatário logo após o crescimento do cabelo. Esse mecanismo oferece uma certa segurança, porém, se o mensageiro for interceptado e revistado a mensagem poderá ser descoberta.

Sendo assim, houve a necessidade de tornar a mensagem incompreensível, para que mesmo com a interceptação do mensageiro seu conteúdo não fosse revelado, contribuindo assim, para o surgimento da Criptografia.

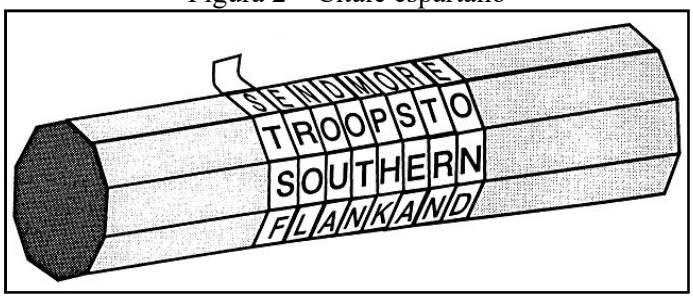
As palavras mais comuns utilizadas na Criptografia são códigos e cifras, no qual código significa substituição de palavras ou frases, e cifras, substituição de letras. Codificar significa ocultar uma mensagem usando códigos e decodificar significa traduzir uma mensagem codificada. De modo análogo, cifrar consiste em misturar uma mensagem utilizando-se cifras

e decifrar, em traduzir a mensagem cifrada. Já encriptar e decriptar são termos mais gerais e englobam os processos de codificação e decodificação dos códigos e das cifras.

> [...] a Criptografia pode ser dividida em dois ramos, conhecidos como transposição e substituição. Na transposição, as letras das mensagens são simplesmente rearranjadas, gerando, efetivamente, um anagrama. Para mensagens muito curtas, tais como uma única palavra, este método é relativamente inseguro porque existe um número limitado de maneiras para se rearranjarem poucas letras. Por exemplo, uma palavra com três letras só pode ser rearranjada de seis maneiras diferentes (SINGH, 2001, p. 23).

Outra forma de transposição é o método que utiliza o citale espartano (primeiro aparelho criptográfico militar), composto por um bastão de madeira (citale) no qual é enrolada uma tira de couro ou pergaminho contendo uma mensagem que desenrolada apresenta uma sequência aleatória de letras (Figura 2). A mensagem só será revelada quando enrolada em torno de um outro citale de mesmo diâmetro.

Figura 2 – Citale espartano



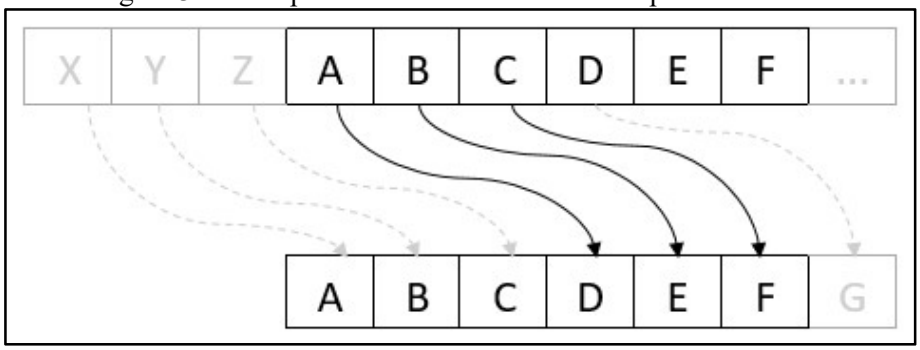
Fonte: Singh (2001, p. 24).

Já na cifra de substituição, cada letra do texto é substituída por uma letra diferente, ou seja, as letras mudam de identidade mantendo a posição, diferentemente da cifra de transposição em que as letras mantêm sua identidade alterando apenas sua posição.

O primeiro registro de utilização do método de substituição foi a cifra usada por Júlio César[3], a cifra de César, que consiste em deslocar o alfabeto em uma determinada quantidade de casas à frente (Figura 3). Essa especificação (quantidade de casas à frente) é conhecida como chave, que define o alfabeto cifrado exato que será usado na codificação.

[3] Político e militar romano (49 a. C. – 48 a. C.). Conquistou com o apoio do Senado os títulos de Pontífice Máximo e Ditador Perpétuo. Informação obtida em: <https://www.ebiografia.com/julio_cesar/>. Acesso em: 27 ago. 2017.

Figura 3 – Exemplo de deslocamento utilizado por Júlio César



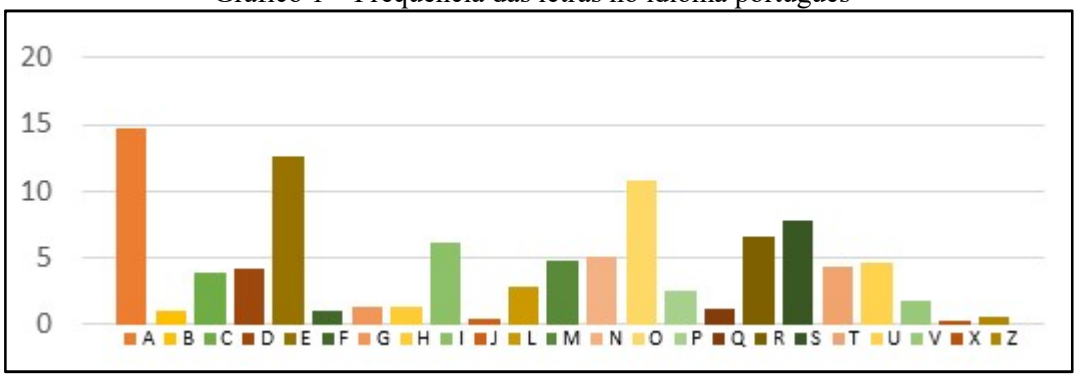
Fonte: Elaboração própria.

Por outro lado, para decifrar uma mensagem, também é necessário o conhecimento da chave utilizada no processo de cifragem. Já a quebra, ocorre quando se obtém a mensagem original sem a utilização dessa chave, como por exemplo, verificando-se todas as possíveis chaves até encontrar a correta. Este método é conhecido como ataque de força bruta.

Muitos estudiosos achavam que a cifra de substituição era inquebrável devido ao grande número de chaves envolvidas, contudo, surge a Criptoanálise, ciência que possibilita quebrar uma mensagem.

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 (Gráfico 1).

Gráfico 1 – Frequência das letras no idioma português



Fonte: Elaboração própria.

O desenvolvimento da análise de frequência fragilizou os processos que até então eram dados como seguros, incitando-se a criação de cifras mais fortes por parte dos criptógrafos. Se por um lado os criptógrafos desenvolvem novos métodos de cifragem, por outro estão os criptoanalistas encontrando formas de enfraquecer esses métodos e quebrar as mensagens, surgindo assim uma batalha que se assemelha à enfrentada pelos médicos com a produção de antibióticos contra as bactérias em sua constante evolução.

> A bactéria vive, se reproduz e prospera até que os médicos descubram um antibiótico que revela uma de suas fraquezas, matando-a. As bactérias são então forçadas a evoluir e superar o antibiótico, e, se forem bem-sucedidas, poderão prosperar de novo e se restabelecer. As bactérias são forçadas a uma evolução contínua de modo a sobreviver ao ataque dos novos antibióticos (SINGH, 2001, p. 12).

Essa batalha entre os criadores e decifradores de códigos contribuiu para o surgimento de cifras mais complexas, como por exemplo, a cifra de Vigenère[4], que consiste em uma tabela (quadrado de Vigenère) formada por 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior (Figura 4). Neste processo, a chave, localizada na primeira coluna, determina a linha que será utilizada para cifrar cada letra, a fileira no topo do quadrado, em letras minúsculas, representa as letras do alfabeto original, e a letra cifrada se encontra na interseção da linha da chave com a coluna da letra original. Sendo assim, a letra *c* será cifrada pela letra L se for utilizada a chave J, que está na fila 9, por exemplo.

Figura 4 – Quadrado 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).

Se utilizar apenas um dos alfabetos cifrados, o processo resulta em uma cifragem simples, como a cifra de César. Contudo, na cifra de Vigenère, cada letra da mensagem é cifrada

[4] O desenvolvimento da cifra de Vigenère teve contribuições do polímata florentino Leon Alberti, do abade alemão Johannes Trithemius, do cientista italiano Giovanni Porta, e do diplomata francês Blaise de Vigenère. Essa cifra leva o nome do homem que a desenvolveu em sua forma final (SINGH, 2001).

em uma linha diferente, e a chave é representada por uma palavra. No processo de cifragem, primeiramente repete-se a palavra-chave acima da mensagem de modo que cada letra da mensagem fique associada a uma letra da chave, e o texto cifrado seja obtido a partir das interseções entre as letras associadas.[5]

Essa cifra foi considerada indecifrável já que uma mesma letra poderia ser codificada de várias formas diferentes, dependendo da quantidade de letras da palavra chave. A força da cifra de Vigenère despertou a curiosidade do britânico Charles Babbage[6], ocasionando sua quebra, apesar desse fato ter sido divulgado anos depois.

Um outro método de cifragem foi a ADFGVX, uma das mais famosas cifras de guerras, adotada por um comitê de criptógrafos, por acreditarem em seu nível de segurança. A força dessa cifra estava em sua natureza complexa, sendo uma mistura de substituição e transposição.

O processo inicia-se com um quadro 6x6, com 36 quadrados, onde são dispostos aleatoriamente 26 letras e 10 dígitos. Cada linha e coluna do quadro é identificada por uma das seis letras A, D, F, G, V ou X (Figura 5).

Figura 5 – Exemplo do quadro da cifra ADFGVX

	A	**D**	**F**	**G**	**V**	**X**
A	8	p	3	d	q	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Fonte: Singh (2001, p. 410).

[5] Como exemplo, utilizaremos a palavra-chave VIDA para cifrar a mensagem QUADRADO. Primeiro, cada letra da palavra-chave deve ser associada a uma letra da mensagem:

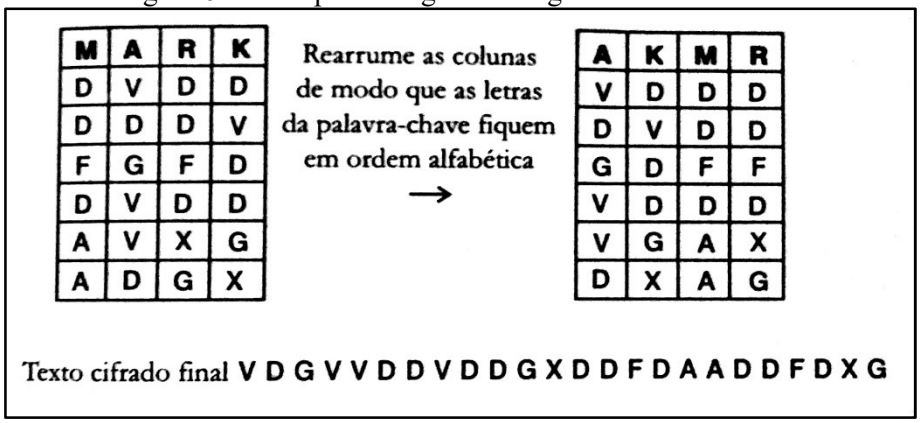
Palavra-chave: V I D A V I D A
Texto original: q u A d r a d O

A letra *q* será cifrada pela letra L utilizando a chave V, localizada na linha 21. A letra *u* será cifrada pela letra C utilizando a chave I, localizada na linha 8. A letra *a* será cifrada pela letra D utilizando a chave D, localizada na linha 3. Assim por diante até obter a mensagem cifrada "LCDDMIGO".

[6] Figura mais intrigante da Criptoanálise no século XIX. Um excêntrico gênio britânico que ficou conhecido pelo seu estudo na construção de uma máquina capaz de calcular tabelas matemáticas sem falhas e com alto grau de precisão (SINGH, 2001).

A cifragem consiste em dois estágios, sendo o primeiro passo identificar a letra que será codificada no quadro e substituí-la pelas letras que representam a linha e a coluna em que está localizada, por exemplo, a letra *p* será substituída por AD. O segundo, consiste em escolher uma palavra-chave, que deve ser do conhecimento do destinatário, que determinará a posição das letras no texto codificado. As letras da palavra-chave são escritas no topo de uma nova grade, e as letras cifradas no primeiro estágio são escritas embaixo, em uma série de linhas. As colunas da grade são rearranjadas de forma que as letras da palavra-chave fiquem em ordem alfabética, obtendo a mensagem cifrada (Figura 6).

Figura 6 – Exemplo do segundo estágio da cifra ADFGVX



Fonte: Singh (2001, p. 410).

Durante a Primeira Guerra Mundial os alemães usavam a ADFGVX por acreditar em sua segurança, porém Georges Painvin[7] decifrou uma mensagem que utilizava essa cifra, proporcionando vantagem aos criptoanalistas sobre os criptógrafos.

> Nos anos posteriores à Primeira Guerra Mundial, com todos os seus fracassos criptográficos, continua a busca por um sistema pratico que pudesse ser usado no conflito seguinte. Felizmente, para os criptógrafos, não demorou muito para que se fizesse uma descoberta, algo que restabeleceria a comunicação secreta no campo de batalha. De modo a reforçar suas cifras, os criptógrafos foram forçados a abandonar a abordagem do papel e do lápis e explorar a tecnologia mais avançada para mandar mensagens (SINGH, 2001, p. 143).

Surge então, a primeira máquina criptográfica, datada do século XV, criada por Leon Alberti[8]. Essa máquina, composta por dois discos de cobre unidos por um pino, era chamada de disco de cifras (Figura 7). Ao longo das bordas de cada disco, encontra-se gravado o alfabeto e como cada disco move-se de forma independente, as letras podem variar de posição formando

[7] Francês e percebera seu talento para os enigmas criptográficos após o início da Primeira Guerra Mundial (SINGH, 2001).
[8] Arquiteto italiano, é considerado um dos pais da cifra polialfabética, ou seja, as cifras que utilizam vários alfabetos cifrados por mensagem (SINGH, 2001).

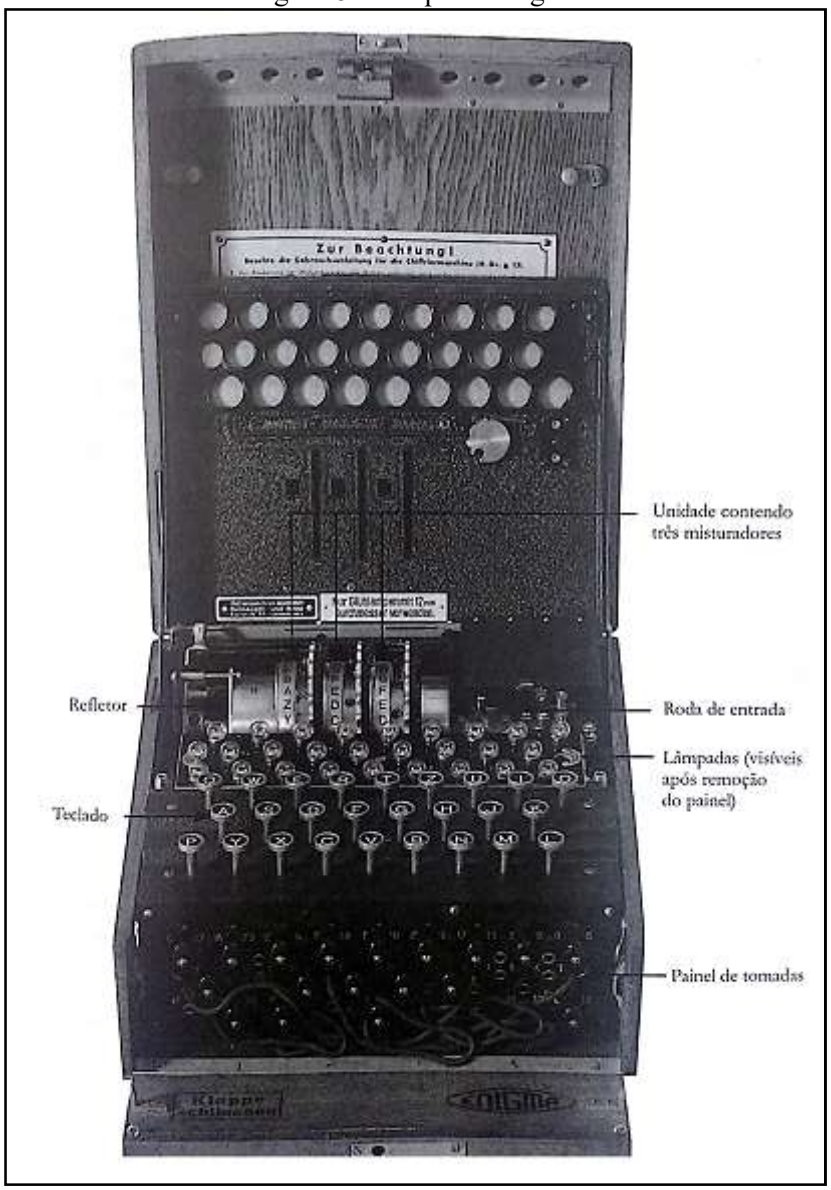
assim cifras de deslocamento, tendo em vista que cada letra da mensagem pode ser cifrada com disposições diferentes do disco. Essa prática pode ser considerada uma forma mecanizada da cifra de Vigenère.

Figura 7 – Disco de cifras

Fonte: Singh (2001, p. 144).

Durante a Segunda Guerra Mundial, os alemães utilizaram uma versão elétrica do disco de cifras de Alberti, a máquina Enigma, para enviar mensagens criptografadas aos seus exércitos. Essa máquina (Figura 8) “se tornaria o mais terrível sistema de cifragem da história” (SINGH, 2001, p. 146).

Figura 8 – Máquina Enigma



Fonte: Singh (2001, p. 159).

Para cifrar uma mensagem utilizando a máquina Enigma, fazia-se necessário ajustes iniciais diariamente na mesma, com base em dados indicados no livro de códigos que era disponibilizado àqueles que faziam parte do grupo responsável pela rede de comunicação nazista.

Já para decodificar uma mensagem, era preciso ter outra máquina Enigma. Além disso, também era necessário possuir o livro de códigos pois sem o mesmo seria impossível configurar a máquina. Isso fazia com que, mesmo em posse da Enigma, os aliados tivessem dificuldade em decifrar as mensagens interceptadas, contribuindo assim para que criptoanalistas buscassem meios de solucionar esse problema.

O polonês Marian Rejewski[9] desenvolveu máquinas, chamadas de bombas, que eram adaptações da Enigma e que foram capazes de verificar os ajustes desta máquina, decifrando assim algumas mensagens. Isto fez com que alemães realizassem modificações na máquina Enigma, ocasionando a desistência dos poloneses nessa disputa pelo fato de não disporem de mais recursos para construção de novas bombas. Mesmo assim, a Enigma mostrou sua fraqueza, deixando de ser considerada perfeita.

Este fato fez com que a Inglaterra convocasse matemáticos, cientistas, linguistas, jogadores de xadrez profissionais, especialistas em palavras cruzadas e em cultura clássica, para decifrarem a Enigma. Essas pessoas foram encaminhadas para Bletchley Park[10], em Buckinghamshire, onde se situava a sede da Escola de Cifras e Códigos do Governo (GC&GS). Dentre eles, destaca-se Alan Turing[11], uma mente brilhante, que, utilizando as descobertas de Rejewski, foi capaz de criar as bombas de Turing e quebrar a cifra da Enigma.

> Durante a Segunda Guerra Mundial os decifradores de códigos britânicos levaram a melhor sobre os fazedores de códigos alemães, porque os homens e mulheres em Bletchley Park seguiram a iniciativa dos poloneses, desenvolvendo algumas das primeiras máquinas de quebra de códigos. 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).

Pode-se afirmar que a máquina Colossus foi a precursora dos computadores modernos digitais pelo fato de ser programável.

Após a Segunda Guerra Mundial, as bombas foram desmontadas, os documentos contendo decifrações destruídos, e os envolvidos dispensados e obrigados a manterem sigilo sobre informações obtidas durante seu período de reclusão. No entanto, depois de três décadas de silêncio, o segredo sobre a quebra da Enigma foi revelado.

A partir daí, os modernos computadores foram utilizados tanto pelos criptoanalistas como pelos criptógrafos. Os criptoanalistas usufruíram de sua velocidade e flexibilidade para

---

[9] Matemático e estudara estatística esperando fazer carreira no ramo dos seguros, mas encontrou sua verdadeira aptidão na quebra de cifras (SINGH, 2001).

[10] Principal estabelecimento de decodificação da Grã-Bretanha durante a Segunda Guerra Mundial, onde cifras e códigos de vários países foram decriptografados, incluindo, as cifras geradas pelas máquinas alemãs Enigma e Lorenz. Informação obtida em: <http://www.bbc.co.uk/history/places/bletchley_park>. Tradução dos pesquisadores. Acesso em: 27 ago. 2017.

[11] Matemático britânico que, em 1939, foi convidado para tornar-se criptoanalistas em Bletchley. Turing foi reconhecido por outros criptoanalistas como um decifrador de códigos com um dom singular, e se tornou o principal criptoanalistas britânico pelo seu trabalho durante a Segunda Guerra Mundial (SINGH, 2001).

testar todas as chaves possíveis até encontrar a correta, quebrando todo tipo de cifras. Já os criptógrafos exploravam o poder do computador na criação de cifras cada vez mais complexas.

O processo para cifrar uma mensagem utilizando computadores se assemelha as formas tradicionais de cifragem, e difere da cifragem por máquinas, como a Enigma, pela geração de cifras complexas, pela velocidade e por misturar números ao invés das letras do alfabeto.

A princípio, apenas os governantes e os militares possuíam computadores, por isso, eram os únicos que poderiam utilizar a cifragem de mensagem por máquinas. Após alguns anos, os computadores se tornaram mais acessíveis possibilitando a compra e a manutenção deste equipamento pelas empresas. Essas empresas usavam os computadores para cifrar comunicações importantes, como transações bancárias e negociações comerciais.

Contudo, os criptógrafos se depararam com uma nova dificuldade, a padronização da Criptografia, devido ao grande número de empresas com computadores que tornaram as cifragens entre elas difundidas.

> Uma empresa poderia usar um sistema particular de cifragem para garantir a segurança das comunicações internas, mas não poderia enviar uma mensagem secreta para uma organização externa, a menos que o receptor usasse o mesmo sistema de cifragem (SINGH, 2001, p. 272).

Diante disso, uma versão simples de uma cifra conhecida como Lucifer, de Horst Feistel[12], foi adotada como cifra padrão por ser considerada um dos mais poderosos sistemas de cifragem disponíveis comercialmente, sendo batizada de Padrão de Cifragem de Dados (DES – *Data Encryption Standard*). Porém, era necessário que o emissor e o receptor tivessem uma chave em comum para se utilizar a cifra DES, obrigando as empresas a lidarem com outro problema, a distribuição de chaves.

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. Ou seja, antes de duas pessoas partilharem um segredo, era necessário partilhar um outro segredo, a chave.

[12] Emigrante alemão que chegara ao Estados Unidos em 1934 (SINGH, 2001).

Com intuito de solucionar este problema, o criptógrafo Whitfield Diffie[13] e o professor Martin Hellman[14] 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[15] se uniu a eles nessa pesquisa.

É neste cenário que aparecem três personagens fictícios, Alice, Bob e Eva, que se tornaram um padrão nos debates sobre Criptografia. Alice deseja enviar mensagens pessoais para Bob ou vice-versa, e Eva quer interceptá-las.

Uma situação foi proposta para evitar a troca de chaves entre Alice e Bob. Alice coloca sua carta dentro de uma caixa com um cadeado e envia para Bob. Ao receber a caixa, Bob coloca nela seu próprio cadeado e a envia para Alice. Alice receberá a caixa com dois cadeados, retirando em seguida o seu e mandando de volta para Bob. Quando Bob receber novamente a caixa, restará apenas seu cadeado, sendo assim, ele poderá retirá-lo e conseguirá ler a mensagem enviada por Alice. Nesse processo, Eva não conseguiria interceptar a mensagem.

Este modelo de caixa com dois cadeados não funciona na vida real, mas inspirou Diffie e Hellman na 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.

Um campo da Matemática rico em funções desse tipo é a aritmética modular[16], cujo processo de reversão das funções é muito mais difícil do que na aritmética normal. E foi após estudos profundos da aritmética modular e das funções de mão única que Hellman propôs uma estratégia para a escolha de uma chave única sem a necessidade de Alice e Bob se encontrarem ou comunicarem a chave para o outro. Inicialmente, Alice e Bob escolhem uma função de mão

[13] Nasceu em 1944 em Nova York, se formou em Matemática no ano de 1965, e passou por uma série de empregos relacionados com segurança em computadores. Diffie sempre demonstrou seu fascínio pelo problema da distribuição de chaves, registrando-o em seu livro de notas intitulado "Problema para uma teoria ambiciosa da criptografia" (SINGH, 2001).

[14] Professor da Universidade de Stanford na Califórnia, nasceu em 1945, num bairro judeu do Bronx. Seu interesse pelas cifras surgiu na infância, e no início de sua pesquisa, encontrou o livro "The Codebrakers" do historiador David Kahn, que serviu de estimulo para se tornar um criptógrafo (SINGH, 2001).

[15] Intelectual que fazia parte de outro grupo de pesquisadores. Juntou-se a este novo grupo pela falta de apoio em seu sonho de resolver o problema da distribuição de chaves (SINGH, 2001).

[16] Conhecida como aritmética dos fenômenos periódicos, cuja principal característica é a repetição em intervalos regulares. Como exemplo, temos o calendário em que a cada sete dias repete-se o mesmo dia da semana. Se dia 10 de setembro é uma segunda-feira, então dia 23 do mesmo mês será um domingo, pois 23-10=13. Considerando que a semana tem sete dias, é possível escrever: 23-10=7+6, o que nos garante que dia 23 de setembro será uma segunda-feira acrescida de seis dias, o que resulta num domingo. Sistematizando, temos que sete é chamado de módulo (n), b pode ser representado por 23 ou 10 e a por 2 ou 3, que são, respectivamente, os restos da divisão desses números por 7. Define-se assim: $a \equiv b \pmod{n}$, em que: a é congruente a b módulo n se $a-b$ é um múltiplo de n (COUTINHO, 2014).

única qualquer, como por exemplo $7^x (mod\ 11)$, e realizam o processo para estabelecer a chave secreta (Figura 9).

Figura 9 – Esquema proposto por Hellman

	Alice	Bob
Fase 1	Alice escolhe um número, digamos 3, e o mantém em segredo. Vamos chamar de *A* o número dela.	Bob escolhe um número, digamos 6, e o mantém em segredo. Vamos chamar de *B* o número dele.
Fase 2	Alice introduz o 3 na função de mão única e o resultado de 7^A(mod 11): 7^3(mod 11) = 343(mod 11) = 2	Bob introduz o 6 na função de mão única e o resultado de 7^B(mod 11): 7^6(mod 11) = 117.649(mod 11) = 4
Fase 3	Alice chama o resultado de seus cálculos de alfa e envia seu resultado, 2, para Bob.	Bob chama o resultado de seus cálculos de beta e envia o seu resultado, 4, para Alice.
A troca	Normalmente este seria um momento crucial porque Alice e Bob estão trocando informações, e portanto esta é uma oportunidade para Eva escutar e descobrir os detalhes da informação transmitida. Contudo, Eva pode ouvir sem comprometer a segurança final do sistema. Alice e Bob podem usar a mesma linha telefônica através da qual escolheram os valores de *Y* e *P*, e Eva pode interceptar esses números que estão sendo trocados, ou seja, 2 e 4. Contudo estes números não são a chave, e por isso não importa que Eva os conheça.	
Fase 4	Alice pega o resultado de Bob e calcula a solução de β^A (mod 11): 4^3 (mod 11) = 64(mod 11) = 9	Bob pega o resultado de Alice e calcula a solução de α^B (mod 11): 2^6 (mod 11) = 64 (mod 11) = 9
A chave	Miraculosamente Alice e Bob terminaram com o mesmo número 9. Esta é a chave!	

Fonte: Singh (2001, p. 290).

Dessa forma, Alice e Bob trocam informações suficientes para a obtenção de uma chave em comum sem que Eva tenha informações necessárias para deduzir o valor dessa chave.

Esse esquema de troca de chaves ficou conhecido como Diffie-Hellman-Merkle e apesar de sua contribuição na história da Criptografia, ele não era perfeito pois ainda existia a necessidade de uma comunicação eficiente entre as duas partes para encontrar a chave.

Diffie então pesquisou uma abordagem diferente para resolver o problema da distribuição de chaves, e idealizou um novo tipo de cifra, que utilizava a chamada chave assimétrica.

Até então, todas as técnicas de cifragem utilizadas eram simétricas, ou seja, a chave era a mesma para cifrar e decifrar a mensagem e o processo de decifragem era oposto ao de cifragem. Já no sistema de chave assimétrica, são duas chaves diferentes: a chave pública (normalmente divulgada para que todos tenham acesso) que é utilizada para cifrar a mensagem, e a chave privada (do conhecimento apenas do destinatário) utilizada para decifrá-la.

Diffie, Hellman e Merkle continuaram sua pesquisa tentando encontrar uma função de mão única para tornar realidade as cifras assimétricas, mas foram outros três pesquisadores que conseguiram criar a cifra mais influente da Criptografia moderna, a cifra assimétrica RSA.

Ron Rivest[17], Adi Shamir[18] e Leonard Adleman[19] desenvolveram a cifra cujo nome representa as iniciais de seus sobrenomes, a RSA, que se baseia em uma função modular da forma $C = M^e \pmod N$, no qual C representa a cifra, M é um número que representa a letra do texto que será cifrado, e é um número qualquer público e N é um número público originado da multiplicação de dois números primos particulares, p e q.

A cifra RSA, também conhecida como Criptografia de chave pública, utiliza uma função de mão única, e sua segurança está no valor de N, pois para que a mensagem possa ser decifrada é necessário o conhecimento dos valores de p e q, que são números primos grandes e difíceis de serem encontrados pela fatoração do número N, que é de conhecimento público.

A Criptografia de chave pública RSA acabou com o problema da distribuição de chaves dando uma clara vantagem aos criptógrafos, porém é possível que no futuro encontrem um modo rápido de fatorar o número N, podendo tornar esta cifra inútil.

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

---

[17] Cientista de computação com uma enorme capacidade de absorver ideias novas e aplica-las em locais improváveis. Sempre atento as novas pesquisas, que serviam de inspiração na busca da chave assimétrica (SINGH, 2001).

[18] Cientista da computação, tinha um intelecto rápido e a capacidade de descartar as informações que não eram relevantes (SINGH, 2001).

[19] Matemático com um enorme vigor, paciência e rigor, sendo responsável por detectar grande parte das falhas apresentadas nas propostas de cifra assimétrica (SINGH, 2001).

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.

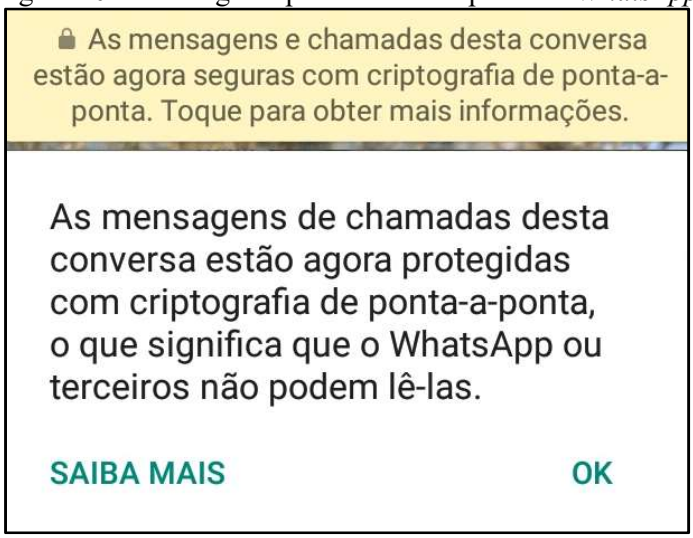
1.1.2 Criptografia na Atualidade

"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).

Muitos aplicativos de celular explicitam o uso da Criptografia como modo de segurança. Um exemplo é o *WhatsApp*, que na página inicial de cada conversa apresenta a seguinte mensagem: "As mensagens e chamadas desta conversa estão protegidas com criptografia de ponta-a-ponta" (Figura 10).

Figura 10 – Mensagem apresentada no aplicativo *WhatsApp*

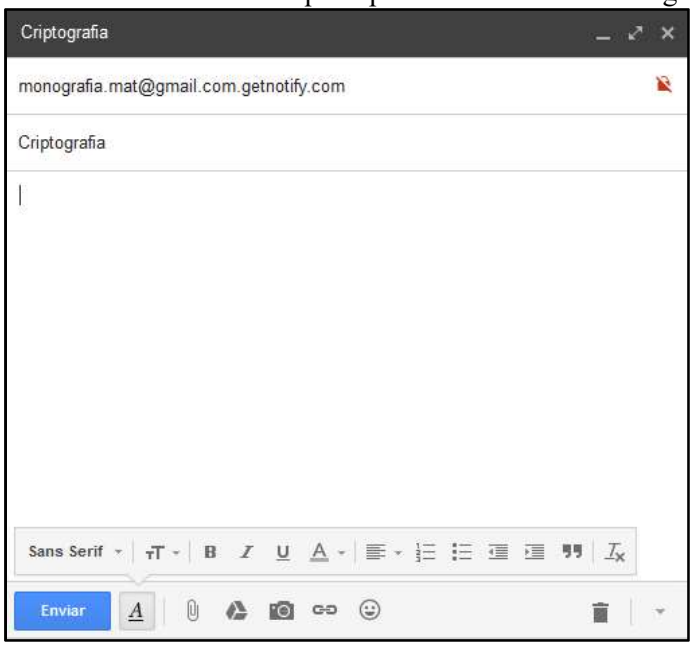


Fonte: Protocolo de pesquisa.

No envio de e-mails, também é possível observar, ao lado direito do campo destinatário, um ícone de cadeado que indica o nível de Criptografia compatível com o destinatário desta mensagem (Figura 11). O cadeado da cor verde representa uma Criptografia avançada, o

cadeado cinza indica a utilização da Criptografia padrão, já o vermelho, aponta que o *e-mail* não é seguro, ou seja, não utiliza Criptografia.[20]

Figura 11 – E-mail com ícone que representa a ausência de segurança



Fonte: Protocolo de pesquisa.

Em outra situação, é possível notar que antes dos endereços de qualquer página na internet aparece a sigla HTTP (*Hyper Text Transfer Protocol*) que significa Protocolo de Transferência de Hipertexto. Quando seguida da letra *s* (HTTPS – *Hyper Text Transfer Protocol Secure*), a sigla passa a significar Protocolo de Transferência de Hipertexto Seguro indicando que a comunicação é criptografada, aumentando significativamente a segurança dos dados (ALVES, 2014).

A Criptografia pode ser encontrada também nas urnas eletrônicas, utilizada em seu *hardware* e *software* por meio da assinatura digital. É uma das mais modernas técnicas quando se trata de Criptografia (BRASIL, s.d.). São utilizados algoritmos dotados de cifração simétrica e assimétrica que são de conhecimento exclusivo do Tribunal Superior Eleitoral (BRASIL, s.d.).

Segundo Dantas (2016), a Criptografia e a Matemática estão interligadas e fazem parte do dia a dia de qualquer indivíduo 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

[20] Informações extraídas do Fórum de Ajuda do Gmail. Disponível em: <https://support.google.com/mail/answer/6330403?visit_id=1-636391975444362694-1890771792&p=tls&hl=pt-BR&rd=1>. Acesso em: 24 ago. 2017.

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 12) 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[21]. A Criptografia é utilizada como auxílio na exploração e aplicação de conceitos matemáticos, tais como números inteiros, aritmética modular e análise combinatória.

Figura 12 – Apostilas da OBMEP

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

1.2 Aprendizagem Significativa

A Matemática tem sido cada vez mais rejeitada pelos alunos por considerá-la uma disciplina difícil. De acordo com Jesus (2011), a dificuldade na aprendizagem de Matemática não está ligada apenas aos conteúdos, mas também envolve a falta de motivação dos alunos por acharem essa matéria desinteressante e sem sentido. Um dos fatores que contribui para essa desmotivação é a dificuldade em vincular os saberes matemáticos escolares às situações cotidianas (JESUS, 2011).

> Percebe-se, então, a necessidade de tornar a Matemática mais interessante para o aluno, de modo que ele tenha prazer em estudá-la. Um dos caminhos possíveis para se alcançar esse objetivo é apresentar a Matemática presente no dia a dia do aluno, fazendo-o perceber que seu estudo é útil e pertinente. Ou seja, é importante contextualizar o ensino (SIQUEIRA, 2016, p.47).

[21] Olimpíada Brasileira de Matemática das Escolas Públicas.

Segundo Kato e Kawasaki (2007), a contextualização do ensino é a associação dos conceitos escolares aos conhecimentos trazidos pelo aluno. Relacionar os conteúdos educativos com os saberes e vivências, facilita a articulação entre a teoria e a prática, permitindo o aluno atribuir sentido e utilidade ao que se aprende (PINHEIRO, 2012). Com isso, Pereira, V. (2012) afirma que, utilizar o conhecimento matemático do cotidiano do aluno na sala de aula, torna as aulas de Matemática mais fascinantes.

Abordar conteúdos de forma contextualizada, proporciona significado ao que é aprendido à medida que este se relaciona a um contexto. Além disso, estimula o protagonismo e a autonomia intelectual do aluno (BRASIL, 2000).

Os documentos que norteiam o currículo nacional do Ensino Médio propõem que o aluno seja capaz de "compreender conceitos, procedimentos e estratégias matemáticas, e aplicá-las a situações diversas no contexto das ciências, da tecnologia e das atividades cotidianas" (BRASIL, 2000, p. 96). Pereira, V. ressalta que:

> Ao final do Ensino Médio, espera-se que os alunos tenham condições de usar a Matemática para resolver problemas do cotidiano, com capacidade de modelar fenômenos em outras áreas do conhecimento, e compreendam que a Matemática é uma ciência com características próprias, construída social e historicamente e de fundamental importância para o desenvolvimento científico e tecnológico (PEREIRA, V., 2012, p. 26).

Portanto, faz-se necessário que o professor, ao elaborar suas aulas, busque a utilização de diferentes estratégias de ensino relacionando, sempre que possível, os temas trabalhados com o cotidiano do aluno, no intuito de proporcionar uma aprendizagem com mais significado.

Aprender, segundo Nunes e Silveira (2011), é um processo no qual o sujeito apropria-se de conhecimentos por meio de estratégias, valores, atitudes, habilidades, entre outros. Neste sentido, a aprendizagem "está relacionada à mudança, à significação e à ampliação das vivências internas e externas do indivíduo" (NUNES; SILVEIRA, 2011, p. 11). Estes autores ainda destacam que o aprender possibilita que algo novo se incorpore aos conhecimentos que o aluno já possui.

Nesta perspectiva, a teoria da Aprendizagem Significativa de Ausubel apresenta uma concepção que se assemelha a essa ideia de aprendizagem. Nesta teoria, os conhecimentos prévios dos alunos são fundamentais para ancorar o novo conhecimento. Santos, A. defende que a aprendizagem significativa

> é um processo pelo qual uma nova informação se relaciona com um aspecto relevante da estrutura de conhecimento do indivíduo, ou seja, um novo conhecimento interage com um conhecimento que o aprendiz já possui, assim ele pode aprender cada vez mais nessa interação, de maneira organizada

> estruturando-se então uma aprendizagem significativa para o sujeito aprendente (SANTOS, A., 2015, p.1).

Esse conhecimento específico, existente na estrutura cognitiva de quem aprende é definido por Ausubel como "subsunçor" (MOREIRA; MASINI, 2006). Santos, A. (2015) afirma que o novo conhecimento e o conhecimento que o aluno já possui se complementam, uma vez que o novo enriquece o pré-existente, atribuindo-lhe novos significados.

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 subsunçores presentes na estrutura cognitiva do indivíduo; e o aprendiz deve estar disposto a aprender.

Este trabalho utiliza o tema Criptografia como o novo material, a fim de contextualizar o ensino de função afim e sua inversa, definidos como subsunçores neste processo, visto que são conhecimentos que o público alvo dessa pesquisa já possui.

Micotti (1999) afirma que aplicar os aprendizados em contextos distintos dos quais foram adquiridos, exigem mais do que a simples mecanização, exigem também domínio de conceitos, flexibilidade de raciocínio, capacidade de análise e abstração. Sendo assim, buscou-se neste trabalho, fazer a contextualização por meio da relação entre a Matemática e a Criptografia, afim de tornar o estudo de função afim e sua inversa mais significativo.

1.3 Trabalhos Relacionados

Para aprofundar o estudo, pesquisas foram realizadas na internet utilizando palavras-chave tais como: "Criptografia e Matemática", "Criptografia e ensino", entre outras. Dentre os trabalhos encontrados, destacam-se os de Loureiro (2014), Pereira, N. (2015), Litoldo (2016) e Pereira, V. (2012) por sua similaridade com a presente pesquisa.

Estes trabalhos, detalhados nesta seção, sinalizam que a Criptografia é capaz de contribuir para o processo de ensino e aprendizagem de vários temas matemáticos, tornando a aprendizagem mais significativa para o aluno.

1.3.1 Tópicos de criptografia para o ensino médio

O trabalho de Flávio Ornellas Loureiro, "Tópicos de criptografia para o ensino médio", é uma dissertação de mestrado defendida em 2014, que teve por objetivo mostrar como é possível utilizar certos tópicos de Criptografia, incluindo sua história, para trabalhar alguns temas de Matemática abordados em turmas do Ensino Médio (LOUREIRO, 2014). Loureiro

(2014) apresenta uma pesquisa bibliográfica da história da Criptografia, relacionando-a com conteúdos matemáticos, como funções, matrizes e análise combinatória.

Esse trabalho apresenta uma proposta de sequência didática composta por cinco atividades na qual o autor expõe os objetivos, pré-requisitos, recursos metodológicos e metodologia utilizada em cada uma dessas atividades. Essa sequência didática não foi aplicada em sala de aula.

Por fim, Loureiro (2014) destaca que foi possível perceber que a Criptografia é um tema abrangente e atual, e sua história é bem rica e interessante, o que ajuda a atrair a atenção do aluno.

Os pontos em comum com esse trabalho monográfico são: o uso da história da Criptografia para abordar temas matemáticos e o público alvo que foram Ensino Médio. Porém, a sequência didática proposta pelo autor envolve outros temas matemáticos, enquanto esta proposta trabalhará apenas com função afim e sua inversa.

1.3.2 Criptografia: uma nova proposta de ensino de matemática no ciclo básico

Outro trabalho destacado é a dissertação de mestrado de Nádia Marques Ikeda Pereira, intitulada “Criptografia: uma nova proposta de ensino de matemática no ciclo básico”, defendida em 2015, cujo objetivo foi evidenciar a Criptografia como uma forma de enriquecer o ensino da Matemática (PEREIRA, N., 2015).

Em sua pesquisa, Pereira, N. (2015) faz um levantamento de aspectos históricos relevantes da Criptografia, mostrando sua evolução e a importância do seu papel na história da humanidade, além de apresentar a Matemática necessária para o seu desenvolvimento. Apesar de não propor uma sequência didática e não apresentar relato de aplicação, Pereira, N. (2015) associa a Criptografia com temas presentes na grade curricular do Ensino Médio e dos anos finais do Ensino Fundamental, como funções, números primos e aritmética modular.

A autora destaca por fim, que o tema Criptografia se torna enriquecedor para o ensino pelo fato de perpassar por vários fundamentos da Matemática em diferentes níveis de ensino, por auxiliar no desenvolvimento das competências de leitura e escrita por meio da história, colaborar com a interdisciplinaridade e principalmente tornar o aprendizado mais significativo.

O trabalho diverge deste trabalho monográfico pelo fato de não apresentar sequência didática e sua aplicação, e também por abranger outros tópicos de Matemática além da função afim e sua inversa. O principal ponto comum é a utilização da Criptografia para tornar a aprendizagem mais significativa.

1.3.3 As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim

A dissertação intitulada “As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim” tem como autora Beatriz Fernanda Litoldo (2016) e teve por objetivo compreender de que forma atividades envolvendo problemas de Criptografia podem auxiliar os alunos na exploração das ideias associadas à função afim (LITOLDO, 2016).

Esse trabalho é fundamentado na metodologia de pesquisa intervenção e a análise dos dados se aproxima de estudos socioculturais conjuntamente com estudos cognitivos permeados por meio de resolução de problemas e de investigações matemáticas.

A pesquisa apresenta uma discussão e reflexão acerca da relação entre a Matemática e os campos de poderes (social, político, econômico, entre outros), sempre elencando esse entrelaçamento com a constante evolução da Criptografia e sua busca constante de cifras seguras e poderosas.

Litoldo (2016) elaborou uma sequência pedagógica de atividades, contendo problemas criptografados, estruturadas na forma de enigmas envolvendo contos baseados no personagem Sherlock Holmes, de Sir Arthur Conam Doyle, com o intuito de abordar a definição de função afim, bem como suas particularidades: função linear, função identidade e função constante, além de trabalhar com a representação gráfica e a definição de função inversa. As atividades foram aplicadas a um grupo de alunos da primeira série do Ensino Médio de uma escola pública de Rio Claro, em São Paulo.

Os dados foram analisados segundo uma abordagem qualitativa, e coletados por meio de observações e anotações em um diário de campo, filmagens e gravações de áudios dos encontros, entrevistas semiestruturadas e fichas de perguntas como atividade.

Nessa pesquisa, Litoldo (2014) concluiu que os alunos desenvolveram atitudes autônomas durante o processo de aprendizagem, adquirindo posturas investigativas. Essas atitudes contribuíram para a criação e a experimentação de diferentes estratégias de resolução, refletindo nas explorações e investigações realizadas por eles a respeito das ideias associadas ao conceito de função afim.

Essa pesquisa se assemelha com esse trabalho monográfico pelo fato de utilizar a Criptografia para contribuir no ensino de função afim. Um ponto distinto é que Litoldo (2016) constrói o conceito de função afim com os alunos, utilizando a investigação. No presente

trabalho, este conceito é um requisito, uma vez que a ideia principal é contextualizar o ensino de função inversa da função afim.

1.3.4 Ensino de Funções: Uma Abordagem Contextualizada Sobre o Tratamento da Informação no Ensino Médio

"Ensino de Funções: Uma Abordagem Contextualizada Sobre o Tratamento da Informação no Ensino Médio", trabalho de Viviane da Silva Stellet Pereira, é uma dissertação de mestrado que foi defendida em 2012, cujo objetivo é investigar o potencial didático da Criptografia e suas contribuições no ensino de Matemática, utilizando os conhecimentos prévios dos alunos sobre funções (PEREIRA, V., 2012).

Esta pesquisa foi embasada na Teoria da Aprendizagem Significativa de Ausubel e na Teoria da Atividade de Leontiev. Sendo assim, Pereira, V. (2012) elaborou atividades utilizando a Criptografia, que valorizam a análise e a descoberta, de modo a favorecer a construção de conceitos matemáticos e aprofundar conteúdos preexistentes envolvendo função, visando facilitar o processo de ensino e aprendizagem de Matemática.

Esse trabalho foi aplicado em um colégio estadual no interior do estado do Rio de Janeiro, e teve como sujeitos alunos de duas turmas de Ensino Médio, sendo uma de primeira série com 21 alunos, e outra de segunda ano com 20 alunos. As turmas escolhidas são de séries diferentes pois o trabalho foca o estudo das funções afim, quadrática, exponencial e logarítmica. Além disso, essas turmas apresentavam baixo rendimento em Matemática e, com a proposta da pesquisa, pretendia-se auxiliar esses alunos, aprimorando seus conhecimentos sobre funções.

Foram realizados dois encontros em cada turma. No primeiro encontro, foram apresentados alguns conceitos necessários do tema Criptografia e das relações codificar e decodificar. Já no segundo encontro, as atividades favoreciam discussões sobre o domínio e o conjunto imagem de funções e funções invertíveis. Na turma da primeira série, a autora trabalhou as funções afim e quadrática na Criptografia. Na turma da segunda série, abordou as funções exponencial e logarítmica na Criptografia.

De acordo com Pereira, V. (2012), os resultados das análises apontaram que a interação de novas informações com conhecimentos prévios do aluno desempenha papel fundamental para uma aprendizagem significativa e que a Criptografia pode servir como excelente recurso nas aulas de Matemática, tornando-as mais prazerosas.

Esse trabalho é o que mais se assemelha com esse trabalho monográfico, pois utiliza a Criptografia para atribuir significado ao ensino de funções, e é embasado também na Teoria da

Aprendizagem Significativa de Ausubel. Porém, um ponto divergente é que Pereira, V. (2012) não foca apenas no ensino de função afim e sua inversa, como pretende-se fazer nesta pesquisa.

2. ASPECTOS METODOLÓGICOS

Neste capítulo é apresentada a metodologia de pesquisa adotada neste trabalho e a descrição da elaboração da sequência didática, pensada para alunos que já tenham estudado função afim e sua inversa.

2.1 Caracterização da Pesquisa

Com o intuito de averiguar possíveis contribuições da Criptografia para o processo de ensino e aprendizagem de função afim e de sua inversa, organizou-se esse trabalho em dois estágios. No primeiro, desenvolveu-se um estudo exploratório acerca do tema Criptografia, desde sua história até algumas aplicações no cotidiano, e a relação estabelecida com a função afim e sua inversa. No segundo estágio, uma pesquisa do tipo Intervenção Pedagógica, tendo em vista que:

> Tais interferências são planejadas e implementadas com base em um determinado referencial teórico e objetivam promover avanços, melhorias, nessas práticas, além de por à prova tal referencial, contribuindo para o avanço do conhecimento sobre os processos de ensino/aprendizagem neles envolvidos (DAMIANI, 2012, p. 3).

As pesquisas do tipo intervenção pedagógica têm como intuito, de acordo com Damiani et al. (2013), detalhar cada etapa realizada, avaliando-as e produzindo explicações que sejam capazes de justificar seus efeitos, fundamentadas nos dados obtidos e nas teorias adotadas com fundamentação do trabalho.

A pesquisa foi realizada com alunos do Ensino Médio que já haviam estudado função afim e sua inversa. Mais especificamente, optou-se por trabalhar com alunos da 1ª série do Ensino Médio da rede Estadual de ensino, visto que, segundo orientações da Secretaria Estadual de Educação do Rio de Janeiro[22], o tema função polinomial de 1º grau deve ser abordado neste ano de escolaridade. Sendo assim, os pesquisadores realizaram uma pesquisa entre escolas estaduais que abordariam esses conteúdos no período em que deveria ser aplicada a presente proposta pedagógica.

Os instrumentos de coleta de dados foram: questionários, diário de bordo, respostas das atividades propostas.

---

[22] Currículo básico de Matemática da primeira série do Ensino Médio proposto pela Secretaria de Estado de Educação do Rio de Janeiro. Disponível em: <www.conexaoeescola.rj.gov.br/site/arq/matematica-regular-curriculo-basico-1s-ob.pdf>. Acesso em: 29 ago. 2017.

Por ser um meio de investigação formado por questões aplicadas a pessoas para obter informações sobre conhecimentos, interesses, percepções, entre outros (GIL, 2012), optou-se por utilizar o questionário para traçar o perfil dos alunos e diagnosticar a percepção dos sujeitos da pesquisa quanto à contribuição da Criptografia no processo de ensino e aprendizagem de função afim e de sua inversa.

O questionário é composto de questões dos tipos aberta, fechada e mista. Conforme Gerhardt e Silveira (2009), nas questões abertas o entrevistado tem a liberdade para responder à pergunta da forma que desejar, obtendo assim, variedades de respostas. As questões fechadas, são formadas por uma lista predeterminada de respostas, no qual o entrevistado deve escolher aquela que corresponda à que deseja fornecer. Esse tipo de pergunta favorece uma padronização dos dados coletados. Já as questões mistas, abrangem os dois tipos anteriores, pois contém uma lista de respostas predeterminadas seguida de um item aberto, exemplo, "comente", "justifique".

Segundo Gil (2012),

> As respostas a essas questões é que irão proporcionar os dados requeridos para descrever as características da população pesquisada ou testar as hipóteses que foram construídas durante o planejamento da pesquisa (GIL, 2012, p. 121).

O diário de bordo foi utilizado para registrar ações vivenciadas durante a experimentação das atividades propostas, que de acordo com Deslandes et al. (2002), é um instrumento no qual pode ser recorrido a todo momento, contendo percepções, emoções e informações que não são obtidas por meio de outras técnicas.

Os dados coletados nessa pesquisa foram analisados segundo uma abordagem qualitativa, pois de acordo com Creswell (2007) a pesquisa qualitativa focaliza os detalhes e os dados são interpretados caso a caso, desprezando-se generalizações.

Segundo Creswell (2007), a pesquisa de caráter qualitativo ocorre num cenário natural no qual o investigador se desloca ao objeto a ser investigado para desenvolver um nível de detalhes sobre os participantes do estudo, além de necessitar do envolvimento ativo dos participantes. Tal investigação qualitativa, emprega diferentes alegações de conhecimento, estratégias de investigações e métodos de coleta e análise de dados (CRESWELL, 2007).

A pesquisa foi desenvolvida nas seguintes etapas:

- Elaboração de questionários;
- Elaboração das atividades que compõem a sequência didática;
- Realização do teste exploratório;
- Análise dos dados coletados e modificação das atividades;

- Experimentação das atividades;
- Análise das respostas dos alunos para verificar se os objetivos foram alcançados.

2.2 Elaboração da Sequência Didática

A sequência didática é composta de três partes. A primeira parte constitui-se de um questionário inicial (APÊNDICE A), cujo objetivo é traçar o perfil do aluno, e de uma atividade de sondagem (APÊNDICE B) para identificar os conhecimentos prévios dos alunos sobre função afim e sua inversa.

Na segunda parte, é apresentado o tema Criptografia e sua evolução histórica, por meio de explicação oral com o auxílio de *slides* (APÊNDICE C) e trechos de vídeos retirados do canal do *Youtube* "M3 Matemática Multimídia"[23]. O objetivo é proporcionar aos alunos um conhecimento sobre o assunto de forma dinâmica. Esta parte compõe-se ainda da realização de atividades em formato de gincana.

Na terceira e última parte, é feita a relação entre a Criptografia e a função afim e sua inversa por meio de duas atividades. Uma de investigação (APÊNDICE D) realizada em conjunto com os alunos, utilizando o quadro branco e *slides* (APÊNDICE E) para resolução e conferência das respostas; e outra atividade, a de verificação (APÊNDICE F) realizada individualmente. Ainda na terceira parte ocorre a aplicação do questionário final (APÊNDICE G), com o objetivo de obter a percepção dos alunos quanto a abordagem do tema.

2.2.1 Questionário Inicial

O questionário inicial tem como objetivo traçar o perfil do aluno, verificar sua visão a respeito da disciplina Matemática, obter informações sobre seu estudo de função afim e sua inversa e seu conhecimento sobre o tema Criptografia.

Este questionário é composto por doze perguntas, sendo duas perguntas abertas, quatro fechadas e seis mistas, e tem como intuito coletar os seguintes dados: i) nome do aluno; ii) sexo; iii) idade; iv) indicar se estudou o 1º ano do ensino fundamental em escola particular ou pública; v) comentar se tem interesse por Matemática; vi) comentar se considera a Matemática uma disciplina importante; vii) justificar se percebe a utilização da Matemática em seu cotidiano; viii) indicar se já estudou função afim; ix) indicar se já estudou função inversa; x) apontar se foi apresentada uma aplicação de função inversa durante seu estudo; xi) expor se já ouviu falar

[23] Disponível em: https://www.youtube.com/user/matematicamultimidia.

sobre Criptografia; xii) dizer se acredita que exista alguma relação entre a Criptografia e a Matemática.

2.2.2 Atividade de Sondagem

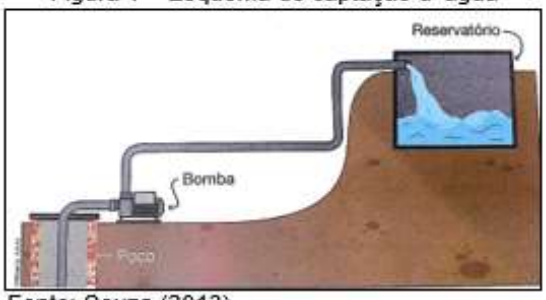
Essa atividade é composta de cinco questões na qual o aluno deve responder usando os conhecimentos adquiridos durante o estudo de função afim e sua inversa ocorrido antes desta intervenção.

A questão um (Figura 13) apresenta um problema envolvendo função afim de forma contextualizada no qual os alunos devem determinar o valor da variável dependente, utilizando a lei de formação da função.

Figura 13 – Questão um da atividade de sondagem

1) (Souza, 2013, p.83 – Adaptada)[1] A água potável utilizada em propriedades rurais, de modo geral, é retirada de poços com auxílio de uma bomba-d'água elétrica. Em certo sítio, para abastecer o reservatório de água, é utilizada uma bomba-d'água com capacidade para bombear 10 litros por minuto. Essa bomba é ligada automaticamente quando o reservatório está com 175 litros de água e desligada ao enchê-lo (Figura 1).

Figura 1 – Esquema de captação d' água



Fonte: Souza (2013).

Com essas informações, podemos escrever uma fórmula que permite calcular a quantidade de água, em litros (ℓ), contida no reservatório em função do tempo (t) em que a bomba permanece ligada, considerando que não haja consumo de água durante esse período.

$$\ell = 10.t + 175$$

Utilizando essa fórmula, calcule a quantidade de água em:

a) 5 min

b) 13 min

Fonte: Elaboração própria.

Na questão dois (Figura 14) os alunos devem determinar as imagens dos valores solicitados, atentando-se para as operações nos itens “b “ e “ c “.

Figura 14 – Questão dois da atividade de sondagem

2) Dada a função f, com $f(x) = 5x + 2$, determine:

a) $f(-1)$

b) $f(0) + f(3)$

c) $f(9) - f(8)$

Fonte: Elaboração própria.

O objetivo das questões um e dois é analisar se os alunos sabem substituir as variáveis pelos valores indicados para obtenção dos resultados.

A questão três (Figura 15) apresenta um problema envolvendo duas grandezas (unidades de tênis vendidas e salário mensal) entre as quais é possível estabelecer uma relação entre elas por meio de uma lei de formação. E, tendo conhecimento do valor de uma das grandezas, espera-se que os alunos determinem o valor solicitado.

Figura 15 – Questão três da atividade de sondagem

3) O salário de um vendedor de tênis é composto por uma parte fixa de R$ 1000,00, mais uma parte variável de R$ 3,00 por unidade vendida. Considerando que o salário do mês de dezembro foi de R$ 1438,00, quantos tênis foram vendidos nesse mês?

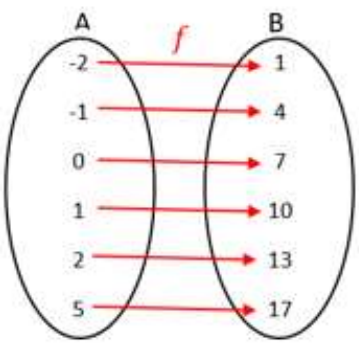
Fonte: Elaboração própria.

O objetivo desta questão é verificar se os alunos são capazes de determinar a lei de formação da função a partir das informações dadas e encontrar o valor pedido.

A questão quatro (Figura 16) requer que os alunos determinem as imagens dos valores dados das funções inversas a partir do diagrama de flechas.

Figura 16 – Questão quatro da atividade de sondagem

4) Seja f uma função afim definida por $f: A \to B$, com A={-2,-1,0,1,2,5} e B={1,4,7,10,13,17}. A partir do diagrama representado a seguir, determine:



a) $f^{-1}(4) =$

b) $f^{-1}(13) =$

Fonte: Elaboração própria.

O objetivo desta questão é analisar a compreensão do aluno sobre o conceito de função inversa.

Na questão cinco (Figura 17) os alunos deverão indicar as funções inversas das funções dadas.

Figura 17 – Questão cinco da atividade de sondagem

5) Determine a inversa de cada função a seguir:

a) $f(x) = 6x - 1$

b) $f(x) = 7x + \frac{2}{3}$

Fonte: Elaboração própria.

Esta questão tem por objetivo analisar a capacidade dos alunos em obter a lei da função inversa a partir da lei de formação da função afim.

2.2.3 Apresentação da Criptografia e sua Evolução Histórica

Esta segunda parte da sequência didática tem como objetivo apresentar os aspectos relevantes da história da Criptografia por meio de apresentação oral, de *slides* ilustrativos e de vídeos curtos.

Optou-se pela utilização do vídeo e do *slide* como ferramentas, pois segundo Moran (1991, p.11), a "utilização do audiovisual para introdução de novos assuntos, desperta a curiosidade e a motivação para novo temas".

Com o intuito de promover a prática dos métodos apresentados sobre o tema Criptografia, são propostas atividades em formato de gincana, que serão pontuadas de forma a se obter um grupo vencedor ao final.

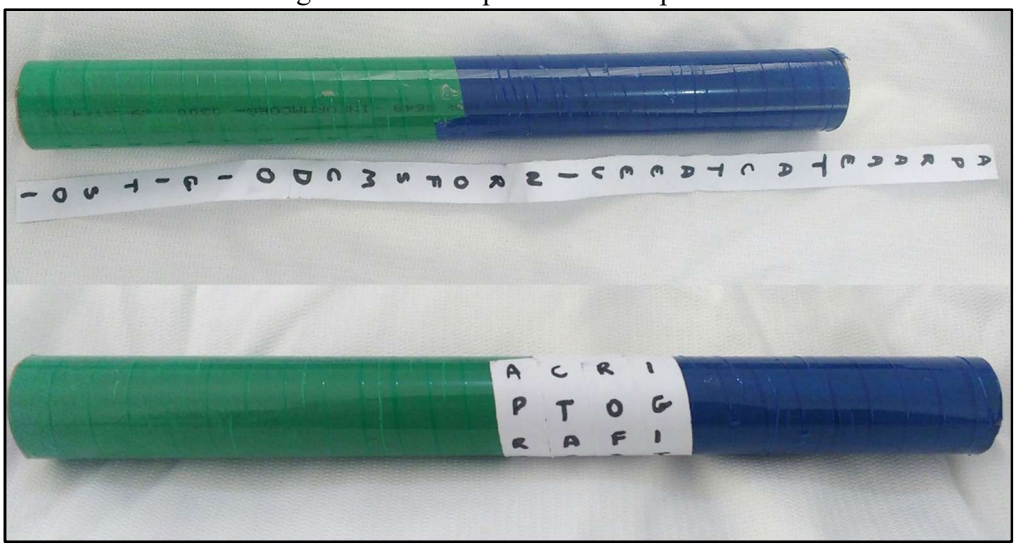
Segundo Oliveira (2010), ensinar de forma lúdica possibilita a construção do conhecimento de forma prazerosa e interessante, garantindo nos alunos a motivação necessária para uma boa aprendizagem. Nesse sentido, Santos, S. (2010) afirma que a utilização de atividades lúdicas na escola é um recurso muito rico, pois proporciona a aquisição de valores já esquecidos, o desenvolvimento cultural e a assimilação de novos conhecimentos, desenvolvendo assim, a sociabilidade e a criatividade.

As atividades realizadas ao longo da aula são individuais, e ao final a turma se divide em quatro grupos para execução das últimas atividades. Em relação ao critério de pontuação, as atividades individuais somam um ponto a cada acerto dos alunos e as em grupo somam 10 pontos por acerto. Os pontos acumulados pelos alunos nas atividades individuais se integrarão

ao somatório do grupo ao qual ele pertencer. A última atividade consiste na abertura de um cadeado, em que as chaves são distribuídas no decorrer da aula para os alunos que terminarem as tarefas primeiro. Todas as atividades são cronometradas para controle do tempo.

A aula se inicia com um questionamento aos alunos sobre o que já ouviram falar sobre Criptografia. Em seguida, é apresentado o vídeo 1, trecho do vídeo "A César o que é de César"[24], contendo a definição de Criptografia, sendo complementado pela explicação do surgimento de sistemas de sigilo nas comunicações. Dois sistemas são citados: a esteganografia, apresentando-se a marca d'água de uma cédula de dinheiro como exemplo, e o citale espartano, apresentando-se como exemplo concreto (Figura 18) em que uma tira de papel com letras aleatórias ao ser enrolado no citale revela a mensagem "A CRIPTOGRAFIA ESTA NO SEU COTIDIANO". O citale foi elaborado pelos pesquisadores, e feito com um tubo de PVC de 1 $^{1}/_{4}$".

Figura 18 – Exemplo do citale espartano

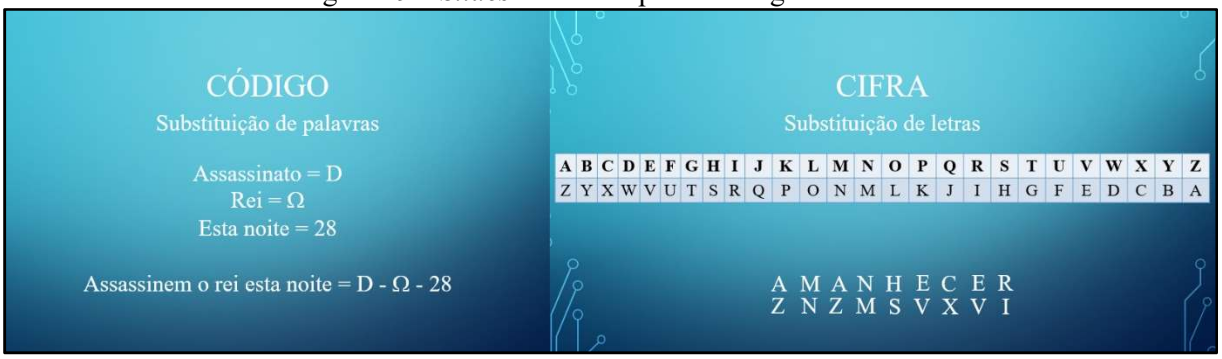


Fonte: Elaboração própria.

Em seguida, é explicada a diferença entre código e cifra com exemplos para melhor compreensão. A frase "Assassinem o rei esta noite" é codificada por "D Ω 28", e a palavra "AMANHECER" é cifrada por "ZNZMSVXVI" (Figura 19).

[24] Disponível em: https://www.youtube.com/watch?v=5mPAmnqlPEs.

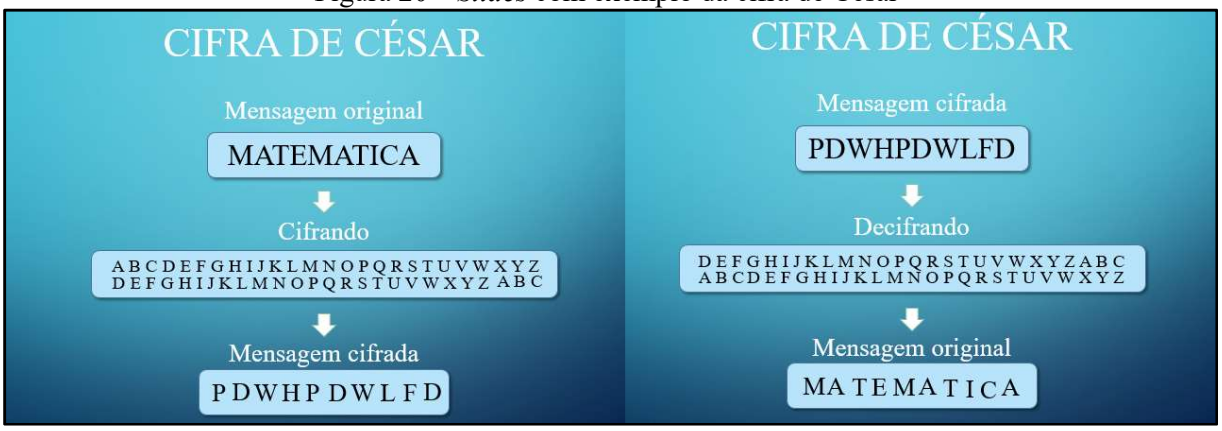
Figura 19 – *Slides* com exemplo de código e de cifra



Fonte: Elaboração própria.

Posteriormente é mencionada a cifra de César utilizada para cifrar a palavra "MATEMATICA", e o procedimento inverso para obter a mensagem original (Figura 20).

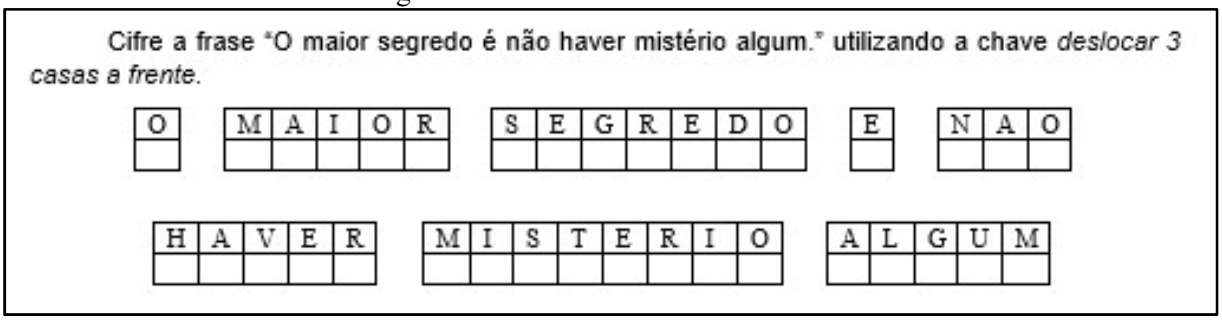
Figura 20 – *Slides* com exemplo da cifra de César



Fonte: Elaboração própria.

Outra atividade é proposta para fixar o processo utilizado por César para cifragem de mensagens (Figura 21). Como citado anteriormente, essa atividade faz parte da gincana, por isso, é distribuída a ficha 1 (APÊNDICE H) para os alunos entregarem com as respostas. É estipulado um tempo de 2 minutos para a realização desta atividade.

Figura 21 – Atividade da cifra de César

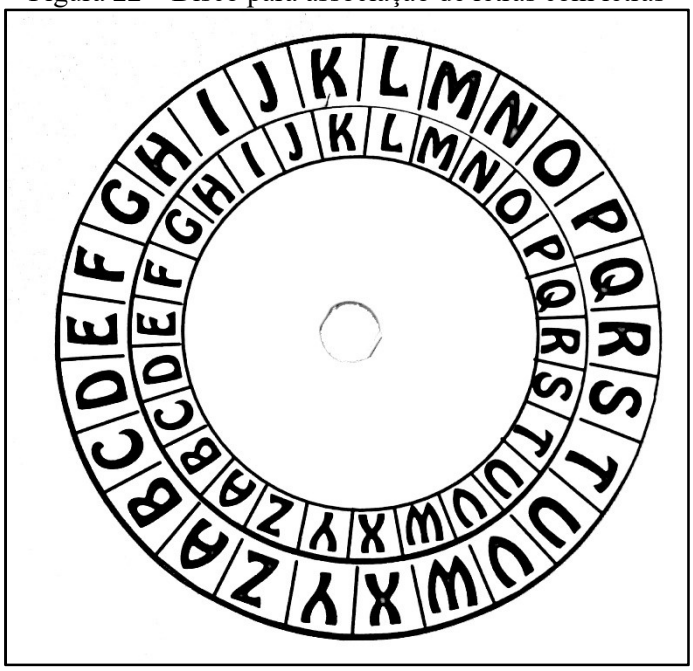


Fonte: Elaboração própria.

Os alunos devem cifrar a mensagem "O MAIOR SEGREDO E NAO HAVER MISTERIO ALGUM" utilizando a chave indicada. Para auxiliar nesse processo são

distribuídos discos de cifras (Figura 22), formados por dois círculos de tamanhos diferentes, em que deve-se mover o menor no sentido horário para avançar, fazendo assim associação de letras. Os discos (APÊNDICE I) foram construídos pelos pesquisadores, em papel branco (180g), inspirado no círculo para criptografar de Malagutti (2015).

Figura 22 – Disco para associação de letras com letras

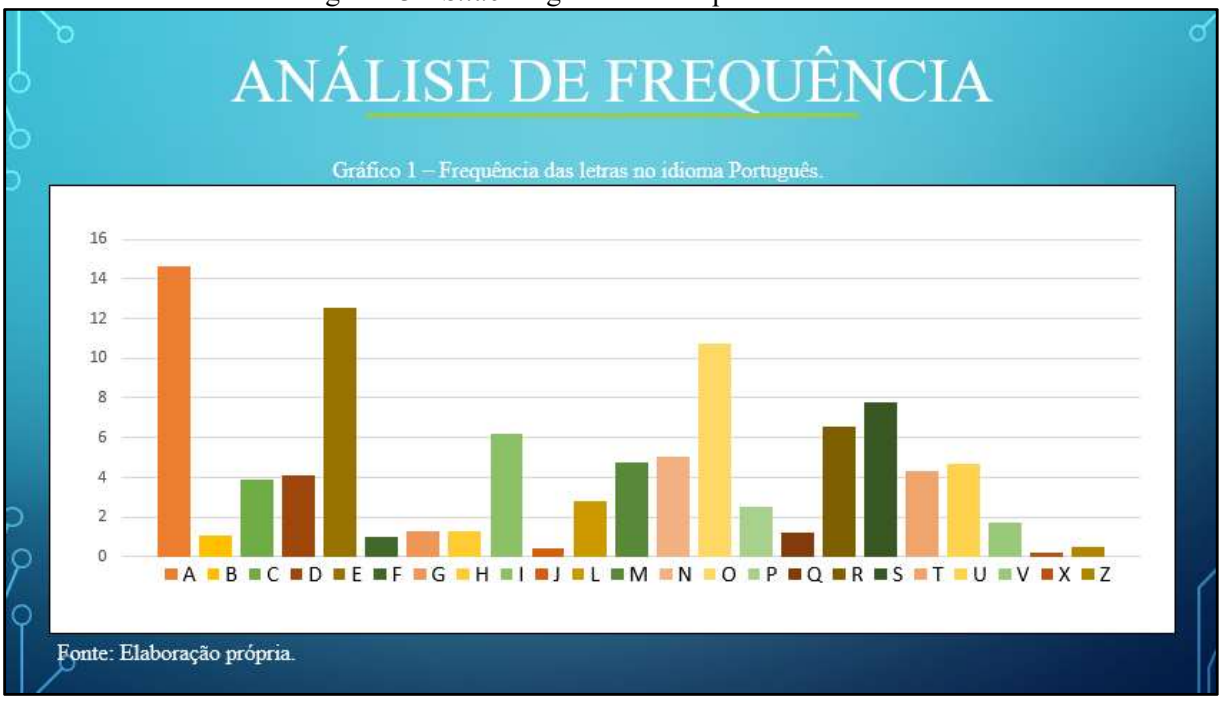


Fonte: Elaboração própria.

A seguir, são apresentados dois tipos de cifra, a de transposição e de substituição, que fazem referência ao citale espartano e à cifra de César, respectivamente, para exemplificação.

Além dos métodos para cifragem de mensagens, existem também métodos que são utilizados para fazer o processo inverso, isto é, decifrar mensagens. Uma breve explicação acerca disso é realizada. Com isso, é apresentada a Criptoanálise para mostrar que é possível obter a mensagem original sem o conhecimento da chave, utilizando a força bruta ou a análise de frequência. Um gráfico de frequência das letras no idioma português (Figura 23) é apresentado para elucidar a técnica de análise de frequência.

Figura 23 – *Slide* do gráfico da frequência das letras

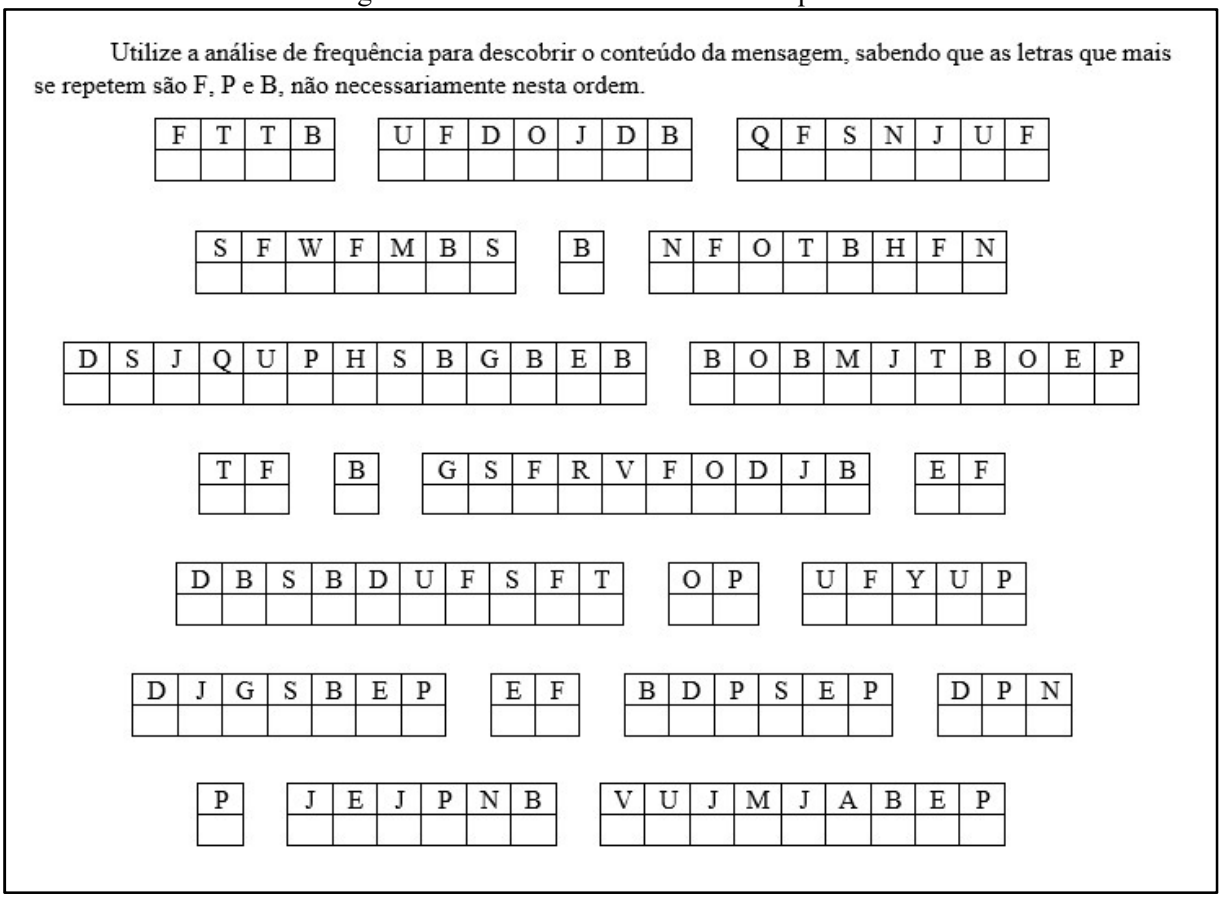


Fonte: Elaboração própria.

O vídeo 2, trecho do vídeo "A loira do banheiro"[25], é utilizado, em seguida, para demonstrar como é feita a análise de frequência e ajudar os alunos na realização da segunda atividade na qual devem obter a mensagem original utilizando este método (Figura 24).

[25] Disponível em: https://www.youtube.com/watch?v=SD_G-kxc3oY.

Figura 24 – Atividade da análise de frequência



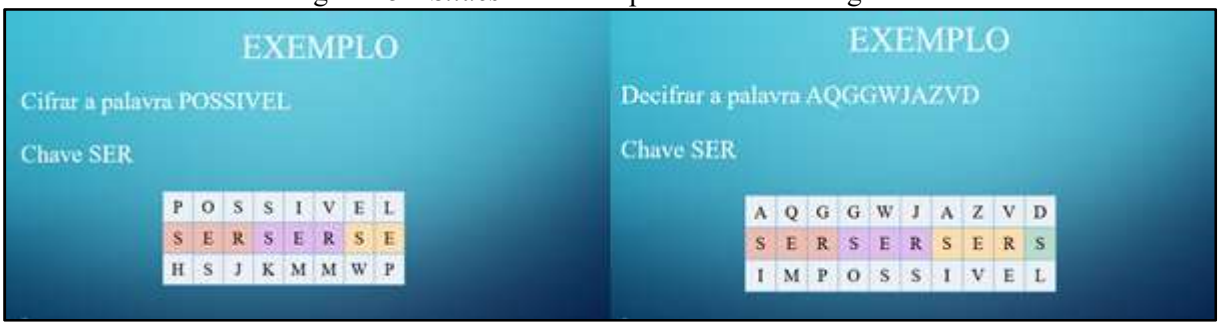
Fonte: Elaboração própria.

A ficha 2 (APÊNDICE J) é entregue aos alunos, e o tempo estipulado para esta atividade é de 5 minutos.

Uma discussão é levantada sobre a disputa que existe entre criptógrafos (aqueles que constroem cifras) e criptoanalistas (os que criam métodos para decifrar mensagens), sendo mencionada a analogia entre o processo que existe entre bactérias e produção de antibióticos com a Criptografia.

Devido a crescente quebra de cifras por parte dos criptoanalistas, cifras mais fortes são criadas a todo momento, como a cifra de Vigenère. Para explicar este método, é cifrada a palavra “POSSIVEL”, obtendo “HSJKMMWP”, e decifrada a mensagem “AQGGWJAZVD”, de modo a se obter a palavra “Impossível”, ambos utilizando a chave “SER” (Figura 25).

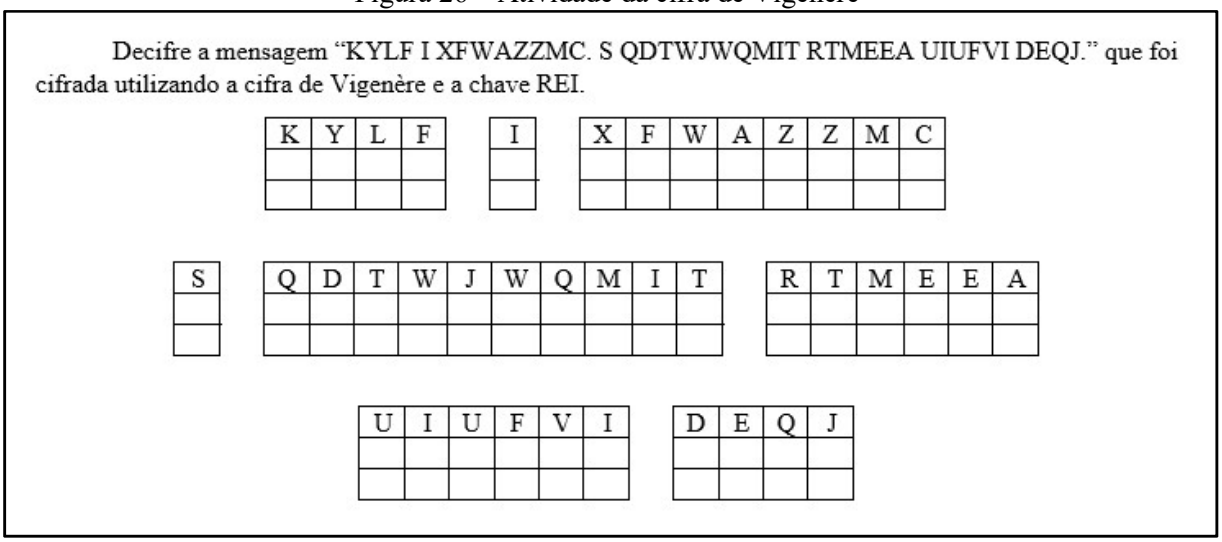
Figura 25 – *Slides* com exemplos da cifra de Vigenère



Fonte: Elaboração própria.

Após explicação deste método, é entregue a ficha 3 (APÊNDICE K) e um quadrado de Vigenère (APÊNDICE L), impresso em uma folha A4, para os alunos realizarem a terceira atividade (Figura 26).

Figura 26 – Atividade da cifra de Vigenère



Fonte: Elaboração própria.

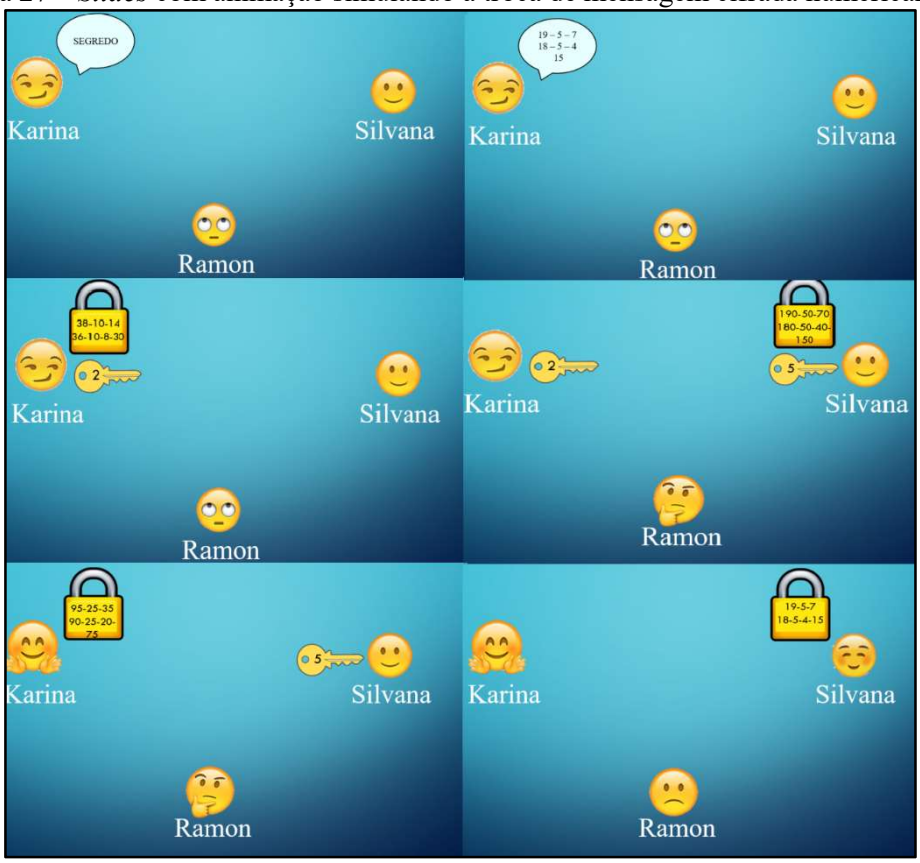
Nesta atividade os alunos devem decifrar a mensagem que foi cifrada utilizando a cifra de Vigenère, com o conhecimento da chave usada. O tempo estipulado para esta atividade é de 5 minutos.

O próximo assunto abordado é a Criptografia na Segunda Guerra Mundial. Para introduzi-lo, é apresentado o vídeo 3, trecho do vídeo "Tempo de Guerra"[26], sobre a máquina Enigma, e uma explicação de seu papel na guerra entre os alemães e os aliados. Logo após, assiste-se um trecho do filme "O jogo da Imitação" [27] (vídeo 4) que mostra o processo que contribuiu para quebra da Enigma.

[26] Disponível em: https://www.youtube.com/watch?v=yzQ_VL8SYQY.
[27] Disponível em: https://www.youtube.com/watch?v=Q2xrQ5U0Tbo.

Com a popularização dos computadores, o problema da distribuição das chaves se tornou mais evidente, e alguns criptógrafos buscaram meios para solucionar este problema. Uma solução apontada por Diffie, Hellman e Merkle se assemelha ao esquema de troca de cadeados, que é apresentado aos alunos por meio do vídeo 5, trecho 1 do vídeo "Venda Segura"[28], sendo complementada por uma animação (Figura 27) produzida pelos pesquisadores, que simula a troca de mensagens cifradas numericamente.

Figura 27 – *Slides* com animação simulando a troca de mensagem cifrada numericamente



Fonte: Elaboração própria.

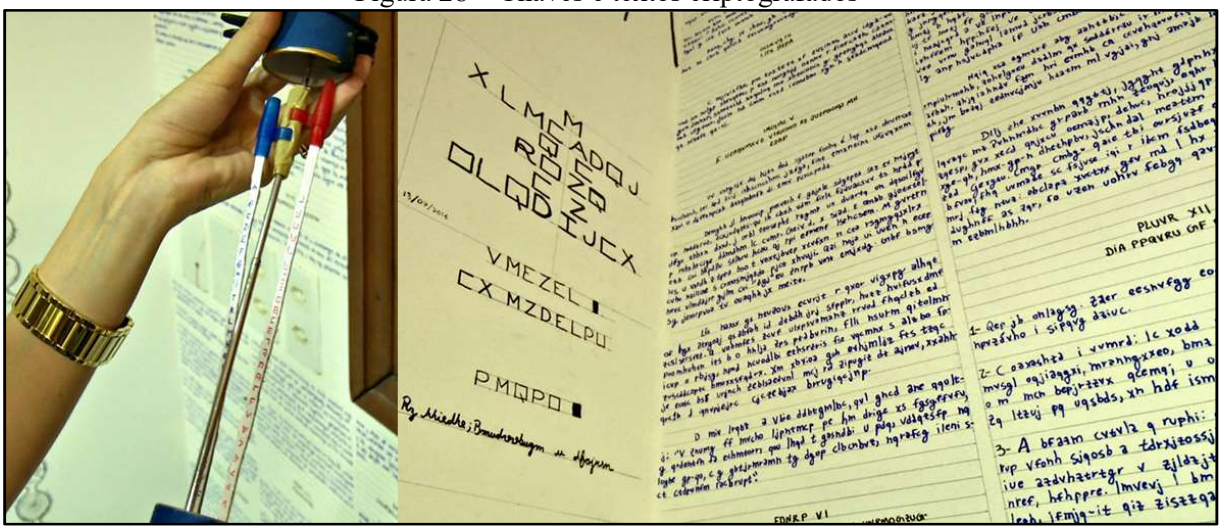
Apesar de não ser eficaz na prática, esse esquema contribuiu para a criação das chamadas chaves assimétricas. Os alunos podem observar a distinção das chaves simétricas com as chaves assimétricas por meio do vídeo 6, trecho 2 do vídeo "Venda Segura".

Ao final, é mencionada a cifra usada hoje em dia, a RSA, que utiliza a aritmética modular por ser uma função considerada de mão única, ou seja, função fácil de fazer e difícil de desfazer. É destacada em seguida, a importância da Criptografia nos dias atuais, e a possível criação de computadores quânticos que podem fragilizar a segurança dos sistemas atuais.

[28] Disponível em: https://www.youtube.com/watch?v=d3b7qE7cnOk.

Um exemplo atual que utiliza Criptografia é citado ao final da aula. Em março deste ano, um caso ocorrido em Rio Branco, no estado do Acre, tomou repercussão nacional. Conforme relatado por Fulgêncio (2017) em um conceituado portal de notícias, foram encontrados no quarto de um jovem desaparecido, 14 livros criptografados além de textos cifrados nas paredes e no teto. O jovem, utilizou vários tipos de cifras, e guardou as chaves dentro de um "canudo" de papelão (Figura 28).

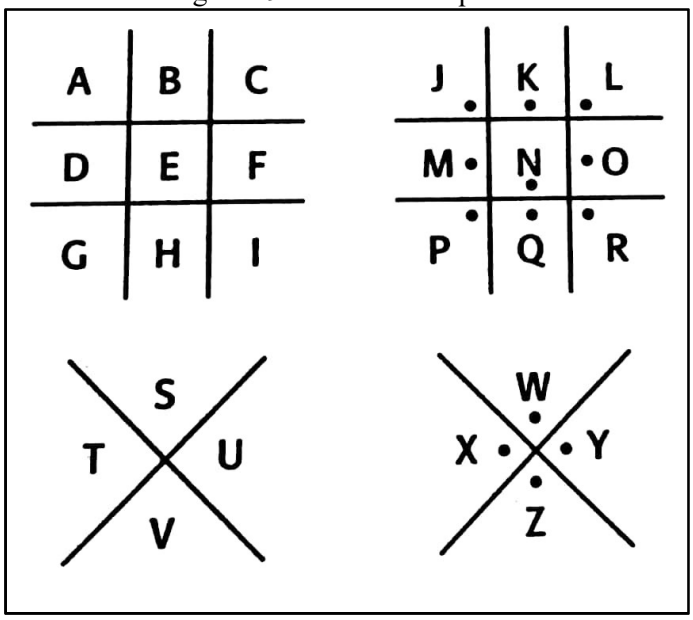
Figura 28 – Chaves e textos criptografados



Fonte: http://migre.me/wpFxz.

Alguns símbolos reconhecidos nas imagens divulgadas, remetem à cifra do chiqueiro. Nessa cifra, as letras são associadas a símbolos de acordo com o padrão apresentado na figura 29.

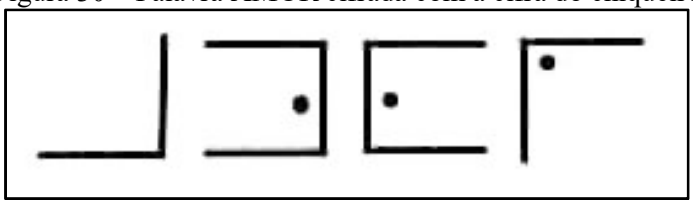
Figura 29 – Cifra do chiqueiro



Fonte: Singh (2001, p. 405).

Para cifrar uma letra, deve-se primeiro encontrar sua posição em uma das quatro grades, e em seguida desenhar a porção da grade que representa aquela letra (SINGH, 2001, p.405). Por exemplo, a palavra “AMOR” seria cifrada como na figura 30, utilizando a cifra do chiqueiro.

Figura 30 – Palavra AMOR cifrada com a cifra do chiqueiro



Fonte: Elaboração própria.

Após citado o caso do jovem, os alunos se dividem em 4 grupos, para realização das outras atividades.

A primeira atividade em grupo se refere a esteganografia e foi baseada no trabalho “Aprendendo Criptologia de Forma Divertida”, de Bezerra, Malagutti E Rodrigues[29]. Nesta atividade, cada grupo recebe uma sequência aleatória de faces contendo números, aparentemente escondidos, e devem encontrar a sequência correta colando em seguida em uma ficha recebida (APÊNDICE M).

O tempo proposto para esta atividade é de 3 minutos, e espera-se que os alunos encontrem a seguinte sequência:

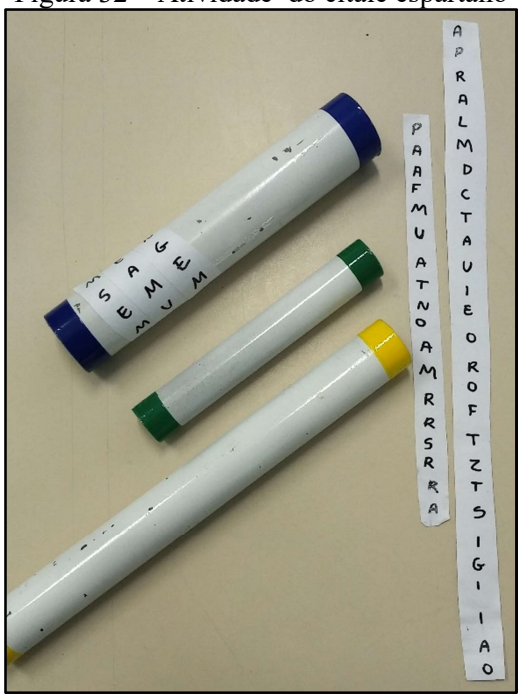
Figura 31 – Sequência das faces

Fonte: Elaboração própria.

A segunda atividade, referente ao uso do citale espartano, cada grupo recebe três bastões de PVC, com diferentes diâmetros e três tiras com letras aleatórias (Figura 32), com o objetivo de descobrir uma mensagem oculta enrolando cada tira de papel no bastão correspondente.

[29] Disponível em: <http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf>

Figura 32 – Atividade do citale espartano



Fonte: Elaboração própria.

Os alunos, ao enrolar as tiras nos citales, devem encontrar a mensagem secreta “A Criptografia utiliza métodos para transformar uma mensagem em um código” e transcrevê-la no verso de uma ficha em formato de cadeado (APÊNDICE N), no tempo de 3 minutos.

A terceira atividade proposta tem como intuito simular a troca de chaves utilizada por Diffie-Hellman-Merkle. Para esta atividade foi elaborada uma planilha do Excel com 5 colunas (Figura 33), em que as mensagens criptografadas (coluna 3) resultam da multiplicação de uma mensagem numérica (coluna 1) e de uma chave também numérica (coluna 2). Para realização desta atividade cada pesquisador fica responsável por um grupo tendo em mãos um *tablet* com a planilha descrita.

Figura 33 – Planilha da atividade de Diffie-Hellman-Merkle

MENSAGEM	CHAVE	MENSAGEM CRIPTOGRAFADA	INFORMAÇÃO DO ALUNO	
15	10	150		0
7	117	819		0
55	37	2035		0

Fonte: Elaboração própria.

Com auxílio dos *tablets*, o responsável passa ao grupo a mensagem criptografada para ser inserida uma chave numérica de sua escolha, que ocorre por meio da multiplicação desse valor pela mensagem recebida. Em seguida, os alunos devolvem a mensagem para que o responsável, ao inserir o valor na coluna 4, retire a chave inserida primeiramente (utilizando a divisão), e retorne para os alunos o resultado (valor que aparecerá na coluna 5), para enfim

retirarem sua chave, também por meio da divisão, e assim obterem a mensagem numérica original. Por exemplo, o responsável passa ao grupo a mensagem criptografada “150” (resultado da multiplicação da mensagem 15 e da chave 10), que irá escolher a chave p e multiplicá-lo pela mensagem, retornando ao responsável a mensagem “150×p”. O responsável retira a primeira chave, ou seja, divide por 10, e passa para os alunos a mensagem “15×p” ($\frac{150\times p}{10}$). O grupo então deve dividir essa mensagem pela chave de sua escolha para retirá-la ($\frac{15\times p}{p}$), e assim obter a mensagem original “15”.

Esse processo ocorre três vezes seguidas até que eles encontrem as três mensagens originais. São distribuídas quatro fichas em formato de chave com sequências diferentes de mensagens (APÊNDICE O), e os grupos devem indicar a chave com a sequência correta, ou seja, a chave que contém a mensagem “15 7 55”. Para esta atividade foi estimado um tempo de 3 minutos.

A última atividade consiste na abertura de um cadeado, por meio do teste de todas as chaves disponíveis, representando o teste de força bruta. Como explicado anteriormente, algumas chaves são distribuídas ao longo das atividades. As que restarem, são divididas entre os grupos. Num total de vinte chaves, apenas uma abre este cadeado. O grupo que tiver posse da chave correta, ganha 10 pontos (Figura 34).

Figura 34 – Chaves e cadeado

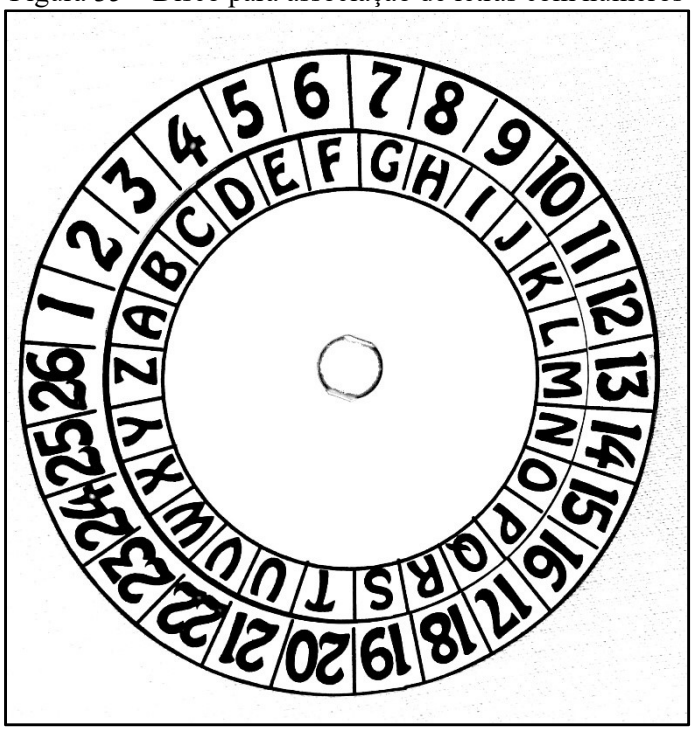
Fonte: Elaboração própria.

O grupo optou por não encerrar a gincana nesta aula para que os alunos continuassem motivados, sendo assim, uma questão da atividade de investigação é realizada em grupo para ser computada na gincana.

2.2.4 Atividade de Investigação

Para estabelecer a relação existente entre a Criptografia com a função afim e sua inversa, foi elaborada uma apostila composta de seis questões. Para introduzir essa relação, os alunos devem primeiramente associar as letras do alfabeto a números. Para facilitar tal associação, é entregue aos alunos um disco (Figura 35) composto de dois círculos, um menor com letras e outro, maior, com números (APÊNDICE P). Neste trabalho, optou-se por associar a letra A ao número 1, a letra B ao número 2, e assim sucessivamente.

Figura 35 – Disco para associação de letras com números



Fonte: Elaboração própria.

Uma explicação é feita sobre a utilização do disco, em que a associação de letras e números ocorre a partir de uma "chave" que dará uma ordem (avance ou recue determinado número de "casas"). É explicado também que o disco estará na posição inicial se a letra A estiver associada ao número 1 e que, a partir de uma chave dada, o deslocamento do círculo menor (sentido horário) é feito a partir desta posição inicial. Um exemplo é se a chave for "avance 4 casas", a letra A fica associada ao número 5. Esse disco fica à disposição dos alunos durante todo o período da aula.

Na questão um (Figura 36), os alunos devem cifrar numericamente o nome da escola, por meio da relação das letras com os números correspondentes, com o auxílio do disco fixado na posição inicial.

Figura 36 – Questão um da atividade de investigação

1) Cifre numericamente o nome da escola.

I	N	S	T	I	T	U	T	O

F	E	D	E	R	A	L

F	L	U	M	I	N	E	N	S	E

Fonte: Elaboração própria.

O objetivo da questão é compreender a associação entre letras e números. Sendo esse o primeiro contato com esse tipo de mecanismo de Criptografia, espera-se que o mesmo seja capaz de encontrar uma mensagem numérica.

A questão dois (Figura 37) retoma a gincana iniciada na aula anterior, sendo a última atividade a ser realizada. Essa questão é adaptada de uma prova da OBMEP de 2007, e proposta para que os alunos a façam com seus grupos.

Figura 37 – Questão dois da atividade de investigação

2) (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: OBMEP, 2007. Adaptada pelos pesquisadores.

Iniciada com um exemplo, a questão propõe no item "a" a cifragem da palavra "OBMEP" utilizando a chave "avance dezenove casas". Nesse momento, os alunos devem usar o disco deslocando o círculo menor no sentido horário, de modo que a letra A fique associada ao número 20. Já no item "b", o aluno deve fazer o processo inverso, decifrando uma mensagem numérica utilizando a chave dada. O item "c" assemelha-se ao anterior, porém antes de decifrar

a mensagem, o aluno deve organizar a sequência numérica criptografada de forma que ao decifrar a mensagem original, obtenha uma palavra com sentido. No último item, o aluno deve encontrar a chave utilizada numa cifragem em que os números correspondentes às letras A, B e C somam 52.

O objetivo da questão dois é reforçar a compreensão dos alunos quanto a associação do alfabeto com os números, a manipulação do disco, assim como possibilitar o desenvolvimento da capacidade do pensar matemático.

Na questão 3 (Figura 38), os alunos devem, utilizando a palavra "CODIGO", indicar a sequência numérica associada, cifrar a palavra CÓDIGO com a chave "avance quatro casas" e, em seguida, escrever a mensagem cifrada. Por fim, com o intuito de introduzir a relação da função afim e o processo de cifragem, espera-se no item "d" que os alunos relacionem a chave cifradora com uma função afim, escrevendo-a segundo a lei de formação $f(x) = x + 4$.

Figura 38 – Questão 3 da atividade de investigação

3) Utilizando a palavra CODIGO:

a) Indique a sequência numérica associada;

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.

O objetivo desta questão é de fixar o processo de cifragem, e além disso compreender que a chave cifradora pode ser escrita como uma lei de formação de uma função afim.

Na questão quatro (Figura 39), os alunos devem cifrar a palavra "CRIPTOGRAFIA" a partir da lei de formação da função. Para isso, devem escrever a sequência numérica associada à palavra dada, substituir cada valor encontrado na lei de formação da função obtendo uma nova sequência numérica e por fim associar cada número dessa sequência a sua letra correspondente.

Figura 39 – Questão quatro da atividade de investigação

4) Cifre a palavra CRIPTOGRAFIA, utilizando a função cifradora $f(x) = 3x + 1$.

Fonte: Elaboração própria.

Ao substituir os valores da sequência numérica na função cifradora, alguns resultados ultrapassam o número 26. Sendo assim, é apresentado um *slide* explicativo (Figura 40) de como proceder nesses casos. O alfabeto é repetido a cada 26 números e a letra que corresponde a um valor acima de 26, é a letra associada ao resto da divisão desse número por 26, acrescida de *n* traços em cima da letra, sendo *n* o quociente da divisão. Por exemplo, se o número obtido na função for 56, temos que o resto da divisão desse número por 26 é 4 e a letra associada ao 56 é a letra D com dois traços em cima ($\overline{\overline{D}}$).

Figura 40 – *Slide* explicativo da associação de letras com números

Fonte: Elaboração própria.

Esta questão tem por objetivo utilizar a função afim como chave cifradora.

Na questão cinco (Figura 41), é proposto aos alunos que decifrem uma mensagem tendo conhecimento da lei de formação da função cifradora da mesma. O objetivo desta questão é permitir a compreensão do uso da função inversa da função cifradora no processo de decifragem da mensagem.

Figura 41 – Questão cinco da atividade de investigação

5) A mensagem TMAC AMLQCESGS foi cifrada a partir da função cifradora $f(x) = x - 2$. Você seria capaz de descobrir a mensagem original?

Fonte: Elaboração própria.

A questão seis (Figura 42), apresenta a função inversa da função que foi utilizada para cifrar a palavra “VESTIBULAR”. Nesse caso, para encontrar a função cifradora, é necessário que os alunos determinem a função inversa da função dada obtendo a função original e, em seguida, fazer o processo de cifragem semelhante ao que foi realizado na questão cinco.

Figura 42 – Questão seis da atividade de investigação

6) A palavra VESTIBULAR foi cifrada utilizando uma função cuja inversa é $f^{-1}(x) = \frac{x-4}{2}$. Qual a função cifradora utilizada, e qual a mensagem?

Fonte: Elaboração própria.

Essa questão tem por objetivo possibilitar ao aluno a compreensão de que a função inversa da função inversa é a função original.

2.2.5 Atividade de Verificação

Essa atividade é composta por quatro questões e tem como principal objetivo analisar se os alunos compreenderam a relação da Criptografia com a função afim e sua inversa, que foi apresentada anteriormente. A atividade de verificação foi elaborada com o intuito de proporcionar autonomia aos alunos para registrar os conceitos apreendidos, sem intervenção dos pesquisadores.

A questão um (Figura 43) foi retirada do vestibular da Fatec de 2017, e optou-se por colocar essa questão para mostrar aos alunos que a Criptografia é um tema que vem ganhando espaço nos Vestibulares e Olimpíadas de Matemática. Essa questão constitui-se de uma tabela incompleta cujo preenchimento deve obedecer a cada um dos itens listados. Em seguida, o aluno deve decifrar a mensagem.

Figura 43 – Questão um da atividade de verificação

1) Questão (Fatec – 2017): Maria, aluna da Fatec Mococa, para garantir a segurança das mensagens que pretende transmitir, criou um sistema de criptografia da seguinte forma:

- montou uma tabela de 2 linhas e 13 colunas para colocar as 26 letras do alfabeto, sem repetição de letra;
- nas cinco células iniciais da 1ª linha, da esquerda para a direita, escreveu, uma a uma, as letras F, A, T, E, C nessa ordem;
- ainda na 1ª linha, na 6ª célula, da esquerda para a direita, obedecendo a ordem alfabética (de A a Z) colocou a primeira letra ainda não utilizada nas células anteriores;
- da 7ª célula a 13ª célula da 1ª linha, inseriu sete letras, da esquerda para a direita, sem repetir letra, seguindo a ordem alfabética, começando pela primeira letra ainda não utilizada nas células anteriores;
- preencheu a 2ª linha, da esquerda para a direita, com as letras restantes do alfabeto, também em ordem alfabética e sem repetição de qualquer letra já utilizada anteriormente.

A tabela mostra o início do processo, com as seis primeiras letras.

F	A	T	E	C	B							

Tendo construído a tabela conforme o descrito, para criptografar uma mensagem, Maria substitui cada letra da 1ª linha pela que está na 2ª linha, na mesma coluna, e vice-versa. A acentuação, a pontuação e o espaço entre as palavras são desconsiderados.

Assim, para desejar BOA PROVA para uma colega, que sabia fazer a decodificação, escreveu RTNEBTHN.

Para João, que também sabia decodificar a mensagem, Maria escreveu:

AGAQNENBPSPNEBPASPB

A partir da decodificação, João entendeu que a mensagem de Maria foi:

a) Nunca pare de aprender
b) Nunca deixe de estudar
c) Nunca faça isso de novo
d) Sempre tire boas notas
e) Sempre faça boas ações

Fonte: FATEC, 2017.

O objetivo principal dessa questão é decifrar uma mensagem que utiliza uma cifra de substituição e espera-se que os alunos completem a tabela de forma correta e por fim decifrem a frase apresentada, substituindo cada letra por sua correspondente até que se obtenham a mensagem original.

A questão dois (Figura 44) inicia-se com a frase “O SEGREDO NÃO SERÁ REVELADO” seguida da chave “avance 5 casas” no qual o aluno deve cifrar esta mensagem e, em seguida, apresentar uma expressão matemática que represente a chave que determina este processo de cifragem.

Figura 44 – Questão dois da atividade de verificação

2) Cifre a frase O SEGREDO NAO SERA REVELADO, utilizando a chave “avance 5 casas”, e indique como a chave cifradora poderia ser escrita em linguagem matemática.

Fonte: Elaboração própria.

Espera-se com essa questão que os alunos utilizem a chave correspondente para cifrar a mensagem dada e, paralelamente, associem esse procedimento a uma expressão que seja correspondente a uma lei de formação de uma função afim.

Na questão três (Figura 45) uma função decifradora é apresentada e a partir daí, os alunos devem cifrar a mensagem “MATEMÁTICA” utilizando a função cifradora, obtida por meio do cálculo da função inversa da função dada.

Figura 45 – Questão três da atividade de verificação

3) A palavra MATEMATICA foi cifrada por João utilizando uma chave cuja função decifradora é $f^{-1}(x) = x - 7$. Qual a função cifradora utilizada, e como ficou a mensagem?

Fonte: Elaboração própria.

O objetivo dessa questão é averiguar a compreensão do aluno de que para obter a função original, basta calcular a função inversa da função inversa dada.

Na questão quatro (Figura 46) são listadas três funções de modo que apenas a função inversa de uma delas possibilita decifrar corretamente a mensagem apresentada, obtendo assim a mensagem “FESTA SURPRESA AMANHÃ A NOITE”.

Figura 46 – Questão quatro da atividade de verificação

4) Henrique recebeu uma carta misteriosa contendo a seguinte mensagem:

TUGFY GEHJHUGY YMYLRY Y LKQFU.

E junto a mensagem havia três funções, das quais uma delas foi utilizada para cifrar a mensagem.

$$f(x) = x + 5$$

$$f(x) = -x + 26$$

$$f(x) = x - 4$$

Qual a mensagem original da carta?

Fonte: Elaboração própria.

O objetivo dessa questão é verificar se os alunos são capazes de calcular a função inversa de cada função dada e de utilizar o pensamento lógico no processo de decodificação aplicado a cada função inversa encontrada, até que se obtenha uma mensagem coerente.

2.2.6 Questionário Final

O questionário final é composto de três perguntas e tem por objetivo captar a percepção do aluno sobre o estudo do tema Criptografia e sua relação com a função afim e sua inversa.

A primeira pergunta se refere ao nome do aluno. A segunda divide-se em duas partes. A primeira parte utiliza a escala de Likert para os alunos assinalarem os itens, de acordo com sua concordância ou discordância, segundo os critérios: D (discordo), DP (discordo parcialmente), NCND (não concordo nem discordo), CP (concordo parcialmente) e C (concordo); e na segunda parte, aberta, há um espaço para comentários e justificativas para os itens assinalados com D, DP ou NCND. Os itens da primeira parte são compostos de afirmações que objetivam ao aluno opinar se o estudo acerca do tema Criptografia: i) foi interessante; ii) agregou novo conhecimento; iii) apresentou relação com conteúdos matemáticos; iv) apresentou linguagem clara; v) foi apresentado de maneira atraente; vi) foi um estudo diferenciado; vii) possibilitou a percepção deste tema no cotidiano; viii) contribuiu no estudo de função afim; ix) contribuiu no estudo de função inversa da função afim; x) tornou o estudo de função inversa mais significativo; xi) permitiu estabelecer relação do tema com a função afim e sua inversa; xii) seria interessante abordar esse tema em sala de aula. A terceira pergunta é aberta, para os alunos relatarem os pontos positivos e negativos a respeito da sequência didática aplicada.

3. RELATO DE EXPERIÊNCIA E ANÁLISE DE DADOS

3.1 Teste Exploratório

O teste exploratório foi realizado nos dias 12 e 13 de abril de 2017 para alunos do segundo período da Licenciatura em Matemática de uma instituição pública do município de Campos dos Goytacazes. A escolha desse grupo deu-se pelo motivo de que esta turma havia realizado recentemente o estudo de função inversa, sendo este um requisito para a aplicação deste trabalho. Tal pesquisa contou ainda com a colaboração de convidados externos e professores da Licenciatura em Matemática. No primeiro encontro estiveram presentes 12 participantes e no segundo, 10. Porém, apenas sete estiveram presentes em ambos os encontros, e destes, um participou como observador. Assim, apresenta-se os dados de seis sujeitos da pesquisa.

A realização do teste exploratório teve por objetivo: i) verificar se a sequência didática estava apropriada para o público alvo pretendido nesse trabalho; ii) analisar o tempo de resolução de cada atividade proposta; iii) averiguar se a linguagem apresentada pelos pesquisadores seria clara e suficiente para compreensão da sequência didática; iv) investigar a clareza e coerência de cada questão; v) estabelecer a quantidade de horários necessários para a realização de cada encontro.

Previamente, foram distribuídos aos convidados e alunos o questionário inicial e a atividade de sondagem, que foram devolvidos no primeiro encontro juntamente com sugestões sobre tais atividades.

A tabela 1 apresenta os dados fornecidos pelos seis participantes no questionário inicial. Vale ressaltar que, mesmo a maioria sendo aluno da Licenciatura em Matemática, todos negaram ter visto aplicação de função inversa.

Tabela 1 – Respostas obtidas no questionário inicial

	Sim	**Não**
Você se interessa por Matemática?	6	0
Você considera a Matemática uma disciplina importante?	6	0
Você consegue perceber a utilização da Matemática em seu cotidiano?	6	0
Já estudou função afim?	6	0
Já estudou função inversa?	6	0
Ao estudar função inversa, foi apresentada alguma aplicação sobre esse tema?	0	6
Já ouviu falar em Criptografia?	6	0
Você acredita que exista alguma relação entre a Criptografia e a Matemática?	6	0

Fonte: Elaboração própria.

A tabela 2 apresenta os resultados obtidos na atividade de sondagem. Das cinco questões propostas, apenas um participante apresentou equívoco na resolução da quinta questão.

Tabela 2 – Respostas obtidas na atividade de sondagem do teste exploratório

	Acerto	**Erro**
1ª Questão – letra a	6	0
1ª Questão – letra b	6	0
2ª Questão – letra a	6	0
2ª Questão – letra b	6	0
2ª Questão – letra c	6	0
3ª Questão	6	0
4ª Questão – letra a	6	0
4ª Questão – letra b	6	0
5ª Questão – letra a	5	1
5ª Questão – letra b	5	1

Fonte: Elaboração própria.

Sobre o questionário inicial, os alunos responderam todos os itens listados, não havendo dúvidas. Na atividade de sondagem duas observações foram feitas: i) trocar a letra de uma das variáveis apresentada na questão 1; ii) incluir a escrita do domínio e contradomínio na questão cinco.

O primeiro encontro (Figura 47) iniciou com uma breve apresentação dos pesquisadores seguida de uma pequena fala ressaltando a importância das observações, das críticas e da participação de cada aluno durante toda realização do teste exploratório. Em seguida, foi apresentada a parte histórica da Criptografia abordando os aspectos relevantes, e paralelamente foram realizadas as atividades individuais sobre a cifra de César, a análise de frequência e a cifra de Vigenère.

Figura 47 – Primeiro encontro do teste exploratório

Fonte: Protocolo de pesquisa.

Pode-se observar que os alunos ficaram totalmente envolvidos durante a explicação, demonstrando ânimo e curiosidade sobre o assunto. Constatou-se que os enunciados das atividades estavam corretos, porém uma observação foi feita: as atividades sobre a cifra de Vigenère e a análise de frequência estavam grandes e cansativas, e por ser um novo conteúdo, frases extensas poderiam desmotivar os alunos.

A seguir, os alunos formaram grupos a fim de responder as outras atividades relacionadas a esteganografia, ao citale espartano, a RSA e ao teste de força bruta (Figura 48).

Figura 48 – Atividades realizadas em grupo

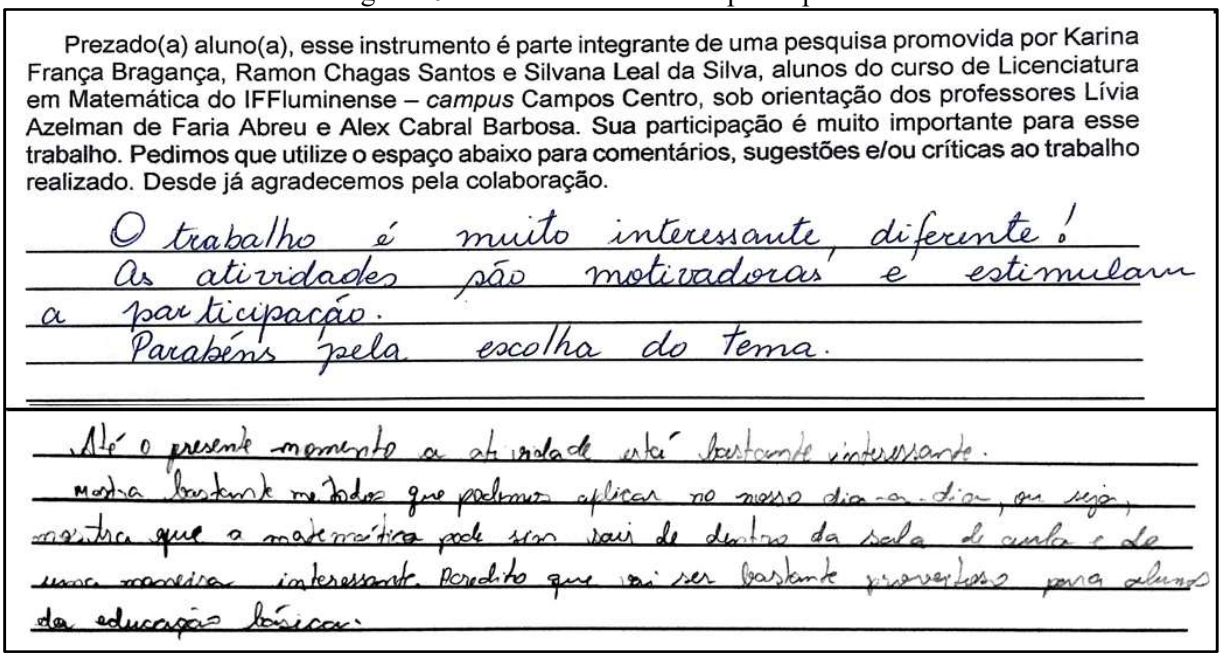
Fonte: Protocolo de pesquisa.

A dinâmica de grupo foi bem aceita entre os participantes, tornando esse momento bastante interativo e dinâmico. Os participantes tiveram interesse em resolver cada umas das atividades propostas e não tiveram dúvida quanto ao desenvolvimento das questões, exceto na atividade sobre a Criptografia RSA em que alguns participantes tiveram dificuldade em entender o procedimento que deveria ser realizado.

Em acordo estabelecido entre os pesquisadores e os orientadores, optou-se por distribuir uma ficha avaliativa aos alunos com o intuito de receber um *feedback* dos mesmos sobre esse

encontro. Obteve-se assim informações importantes sobre a aula (Figura 49), até mesmo de alunos que não poderiam participar do encontro posterior.

Figura 49 – Comentários de dois participantes



Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho. Pedimos que utilize o espaço abaixo para comentários, sugestões e/ou críticas ao trabalho realizado. Desde já agradecemos pela colaboração.

O trabalho é muito interessante, diferente!
As atividades são motivadoras e estimulam a participação.
Parabéns pela escolha do tema.

Até o presente momento a atividade está bastante interessante.
Mostra bastante métodos que podemos aplicar no nosso dia-a-dia, ou seja, mostra que a matemática pode sim sair de dentro da sala de aula e de uma maneira interessante. Acredito que vai ser bastante proveitoso para alunos da educação básica.

Fonte: Protocolo de pesquisa.

No segundo encontro, os pesquisadores iniciaram a aula relatando aos alunos que será apresentada uma relação entre o alfabeto e os números inteiros. Foi distribuída uma apostila aos participantes referente a atividade de investigação. Cada questão foi realizada juntamente com os pesquisadores com o intuito de auxiliá-los, pois até o momento não havia sido feita tal relação.

Os alunos conseguiram acompanhar todas as questões trabalhadas (Figura 50), e os pesquisadores se propuseram a esclarecer as dúvidas que foram surgindo nessa etapa.

Figura 50 – Participantes resolvendo as atividades

Fonte: Protocolo de pesquisa.

A questão dois da apostila (questão da OBMEP-2007) fazia parte da gincana do encontro anterior, sendo assim, a ficha em formato de cadeado foi entregue aos alunos para registro de suas respostas em seu verso e recolhida, para que pudesse ser computado o ponto dessa questão no saldo de pontos do grupo que a acertou.

Em relação a atividade de verificação, pode-se inferir que os resultados coletados (Tabela 3) foram positivos. Os participantes, em sua maioria, não apresentaram dificuldades na resolução das questões propostas. Na primeira e na terceira questão, por exemplo, todos encontraram o resultado.

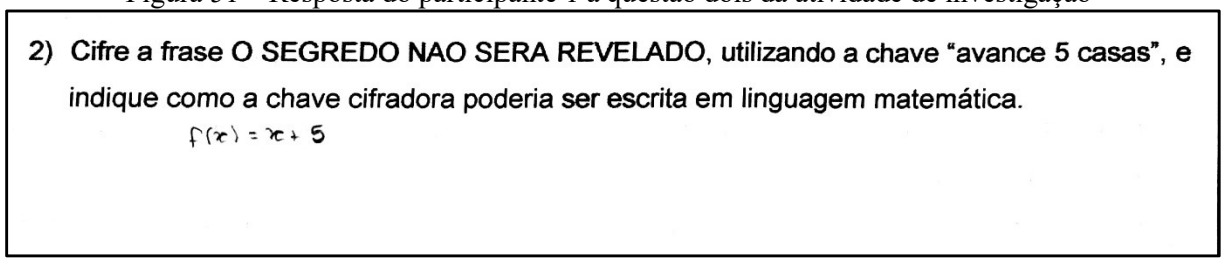
Tabela 3 – Respostas obtidas na atividade de verificação

	Acerto	**Erro**	**Resposta Parcial**	**Em Branco**
1ª Questão	6	0	0	0
2ª Questão	5	0	1	0
3ª Questão	6	0	0	0
4ª Questão	4	0	1	1

Fonte: Elaboração própria.

A respeito da segunda questão, um dos participantes respondeu parcialmente, pois colocou apenas um dos dois itens pedidos (Figura 51).

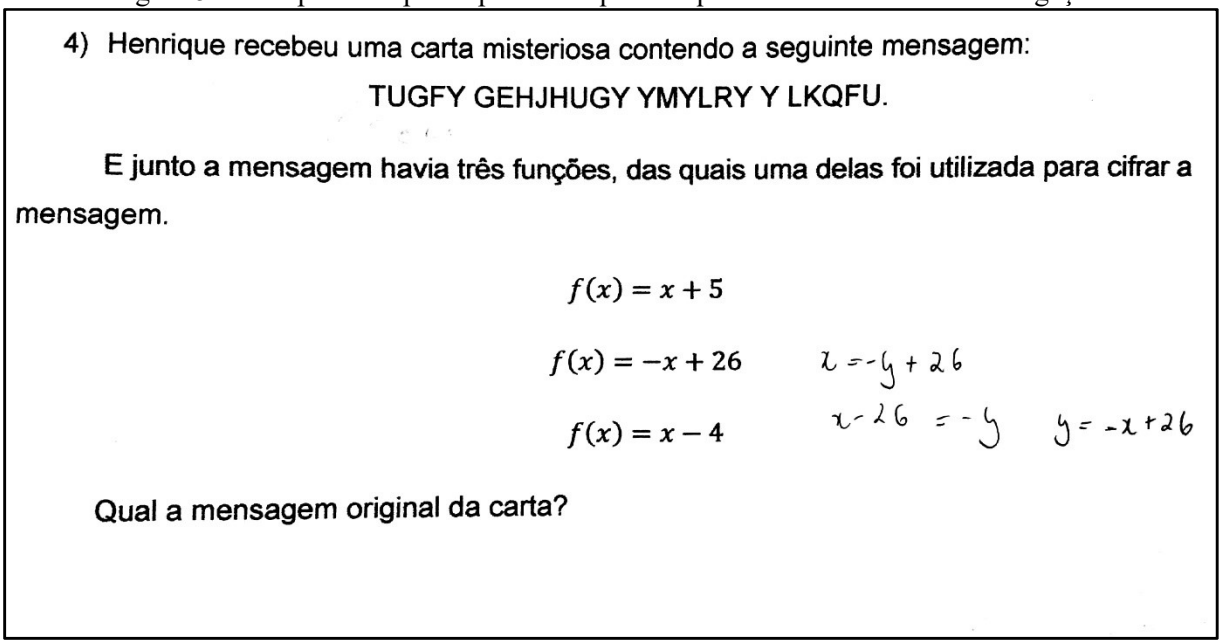
Figura 51 – Resposta do participante 1 à questão dois da atividade de investigação



Fonte: Protocolo de pesquisa.

Na quarta questão, um dos participantes não apresentou registro de resposta e outro participante deixou parcialmente respondido, indicando apenas a função inversa de umas das funções listadas (Figura 52).

Figura 52 – Resposta do participante 2 à questão quatro da atividade de investigação



Fonte: Elaboração própria.

Apesar das respostas incompletas ou ausência de resposta nas questões dois e quatro, optou-se por manter as questões sem alterações, por estarem coerentes com o objetivo da atividade de verificação.

Após esta atividade, foi entregue aos participantes o questionário final com o intuito de obter opiniões sobre a sequência aplicada e considerações em relação aos itens apresentados. A partir de dados coletados (Tabela 4), pode-se inferir que o trabalho estava coerente e tem potencial para responder o objetivo dessa pesquisa.

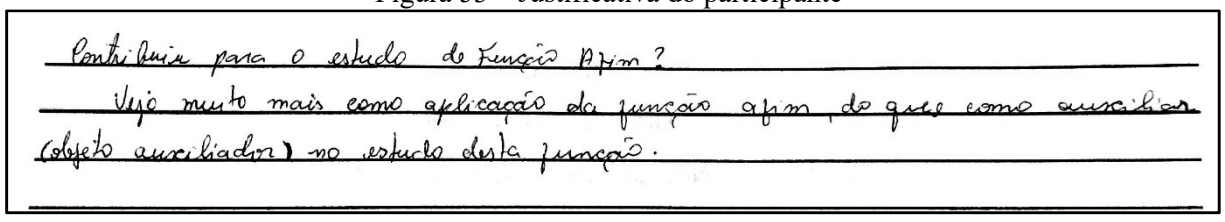
Tabela 4 – Respostas obtidas no questionário final

	D	DP	NC/ND	CP	C
Foi interessante.	0	0	0	0	6
Agregou novo conhecimento.	0	0	0	0	6
Apresentou relação com conteúdos Matemáticos.	0	0	0	0	6
Apresentou linguagem clara.	0	0	0	3	3
Foi apresentado de maneira atraente.	0	0	0	0	6
Foi um estudo diferenciado.	0	0	0	0	6
Possibilitou a percepção deste tema no cotidiano.	0	0	0	1	5
Contribuiu no estudo de função afim.	0	0	1	1	4
Contribuiu no estudo de função inversa da função afim.	0	0	0	0	6
Tornou o estudo de função inversa mais significativo.	0	0	0	1	5
Permitiu estabelecer relação do tema com a função afim e sua inversa.	0	0	0	1	5
Seria interessante abordar esse tema em sala de aula.	0	0	0	2	4

Fonte: Elaboração própria.

Um dos participantes afirmou não concordar nem discordar quanto ao estudo do tema Criptografia contribuir no estudo de função afim. A figura 53 apresenta a justificativa dada por este participante.

Figura 53 – Justificativa do participante



Fonte: Elaboração própria.

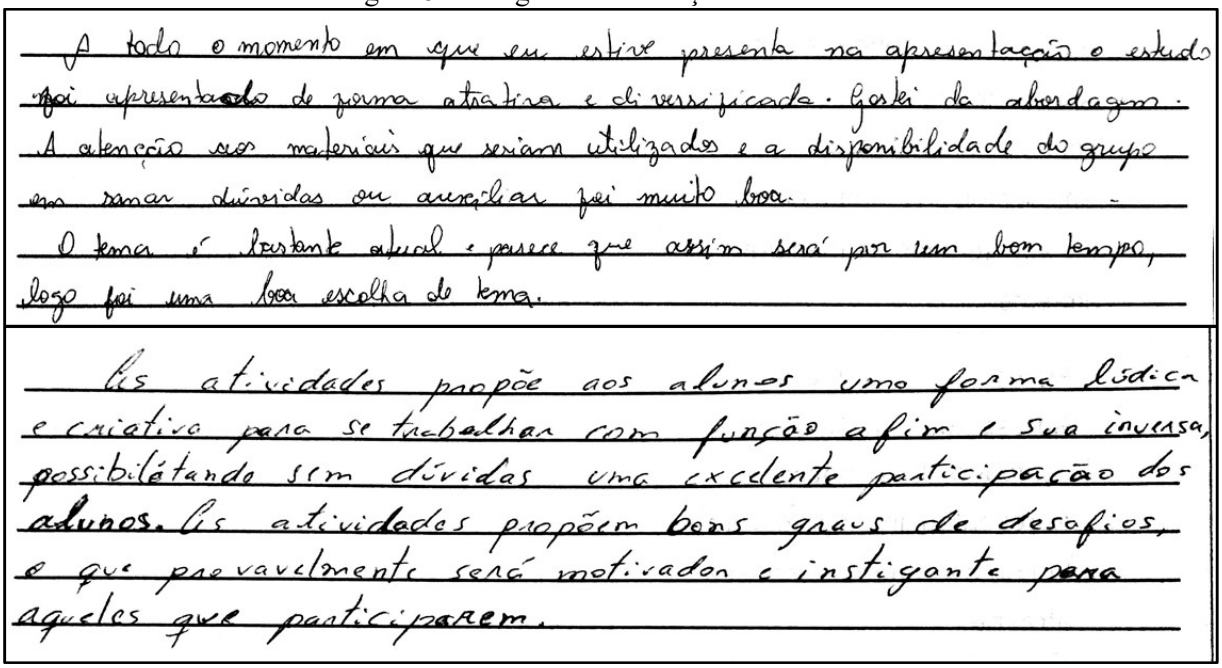
Apesar da afirmação feita, os pesquisadores consideram que ao apresentar uma aplicação de um determinado conceito, há contribuição para o estudo do mesmo, pois como orientam os PCNEM, " a aplicação de conhecimentos constituídos na escola às situações da vida cotidiana e da experiência espontânea permite seu entendimento, crítica e revisão" (BRASIL, 2000).

A respeito disso, Lima (1999) destaca que o ensino de Matemática deve abranger a conceituação, manipulação e a aplicação. Mais especificamente, a aplicação tem papel fundamental nas aulas pois pode justificar o estudo dos conceitos e manipulações, tornando o

estudo mais atrativo para o aluno (LIMA, 1999). Com isso, os pesquisadores entendem que o tema Criptografia como exposto nesta pesquisa, tem potencial para ser utilizado como ferramenta para aplicação de conteúdos que muitas vezes se limitam à estudos de conceitos e manipulações, como o de função inversa.

Também podemos destacar outros comentários em relação ao trabalho (Figura 54).

Figura 54 – Registros em relação ao trabalho.



Fonte: Elaboração própria.

Para finalizar o segundo encontro, foi aberta uma discussão em que os participantes tiveram a oportunidade de expor suas experiências ao longo do trabalho. Em seguida os pesquisadores informaram o resultado da gincana, premiando o grupo vencedor e agradecendo a participação de todos.

Algumas modificações foram feitas na sequência didática a partir do teste exploratório, que serão relatadas na seção a seguir.

3.2 Modificações na Sequência Didática

Após a aplicação do teste exploratório, algumas modificações foram feitas na sequência didática, com o intuito de aperfeiçoá-la para a experimentação na turma regular.

No questionário inicial (APÊNDICE Q), foi alterada a palavra “acredita” por “considera”, na pergunta de número 12 (Quadro 1), devido a sugestão de uma das professoras que participaram do teste exploratório.

Quadro 1 – Pergunta de número 12 do questionário inicial

Antes da alteração
12- Você acredita que exista alguma relação entre a Criptografia e a Matemática? ( ) Sim ( ) Não
Após a alteração
12- Você considera que exista alguma relação entre a Criptografia e a Matemática? ( ) Sim ( ) Não

Fonte: Elaboração própria.

Na primeira questão da atividade de sondagem (APÊNDICE R), foi alterada a letra que representa a grandeza quantidade (Quadro 2).

Quadro 2 – Primeira questão da atividade de sondagem

Antes da alteração
Com essas informações, podemos escrever uma fórmula que permite calcular a quantidade de água, em litros (ℓ), contida no reservatório em função do tempo (t) em que a bomba permanece ligada, considerando que não haja consumo de água durante esse período. $\ell = 10.t + 175$
Após a alteração
Com essas informações, podemos escrever uma fórmula que permite calcular a quantidade (q) de água, em litros, contida no reservatório em função do tempo (t), em minutos, em que a bomba permanece ligada, considerando que não haja consumo de água durante esse período. $q = 10\,t + 17$

Fonte: Elaboração própria.

Já na quinta questão, também da atividade de sondagem, foi acrescentado o conjunto domínio e contradomínio das funções (Quadro 3), devido observações citadas pelos participantes no teste exploratório.

Quadro 3 – Quinta questão da atividade de sondagem

Antes da alteração
5) Determine a inversa de cada função a seguir:
Após a alteração
5) Considerando as funções $f: \mathbb{R} \to \mathbb{R}$ e $g: \mathbb{R} \to \mathbb{R}$, determine a inversa de cada função a seguir.

Fonte: Elaboração própria.

Na apresentação da Criptografia e de sua evolução histórica (APÊNDICE S), os pesquisadores optaram por alterar o exemplo de decifragem da cifra de Vigenère, para facilitar a atividade que os alunos realizam em seguida. Ao invés de decifrar a palavra “IMPOSSIVEL”,

o exemplo propõe decifrar a palavra “MENSAGEM”, dando oportunidade aos pesquisadores de alertar os alunos para o fato de que, ao cifrar ou decifrar a letra *a*, deve-se levar em consideração a primeira coluna do quadrado de Vigenère.

Outra modificação na apresentação da parte histórica foi o acréscimo de *slides* com imagens de sistemas que utilizam a Criptografia hoje em dia, e outro com explicação da cifra do chiqueiro, por recomendação de outra professora que também participou do teste exploratório alegando melhor organização da apresentação. Além disso, a explicação da aritmética modular foi retirada da apresentação, pois não é de interesse dos pesquisadores aprofundar esse tema.

Em relação as atividades individuais da gincana, houve redução das frases usadas nas atividades de análise de frequência (APÊNDICE T) e da cifra de Vigenère (APÊNDICE U). O tempo de realização de algumas atividades também sofreu alteração. A atividade da cifra de César passou de 2 para 5 minutos, e a de análise de frequência passou a ser de 10 minutos ao invés de 5.

Nas atividades da gincana realizadas em grupo, optou-se pela retirada da questão sobre a distribuição de chaves (questão que utilizava o *tablet*), tendo conhecimento de que a atividade é de alta complexidade e que poderia não atingir o objetivo dos pesquisadores.

As fichas entregues para as atividades da cifra de César (APÊNDICE V) e esteganografia (APÊNDICE W), sofreram alterações apenas no título, pois antes eram destinadas ao teste exploratório passando agora para experimentação.

Alguns participantes questionaram a utilização do cronômetro e a forma de distribuição de chaves. No entanto, os pesquisadores entendem que é importante utilizar o cronômetro para controle do tempo das atividades. Preferem também manter a regra anteriormente adotada para distribuir as chaves, já que é uma forma de premiar os participantes que encerram primeiramente as tarefas, e a pontuação para quem as realizam corretamente.

Na primeira questão da atividade de investigação (APÊNDICE X) em que é solicitado cifrar o nome da escola, no teste exploratório foi usado o nome do Instituto Federal Fluminense, enquanto na experimentação tem o nome da escola onde a mesma ocorreu. Já a questão da OBMEP, que anteriormente era a segunda questão, passou a ser a última questão.

Ainda na atividade de investigação, foi acrescentado nas questões quatro, cinco, seis (que passaram a ser as questões três, quatro e cinco, respectivamente) os conjuntos domínio e contradomínio das funções (Quadro 4), o que possibilita aos alunos a percepção dos valores que satisfazem a condição dada.

Quadro 4 – Questões da atividade de investigação

Antes da alteração
4) Cifre a palavra CRIPTOGRAFIA, utilizando a função cifradora $f(x) = 3x + 1$. 5) A mensagem TMAC AMLQCESGS foi cifrada a partir da função cifradora $f(x) = x - 2$. Você seria capaz de descobrir a mensagem original? 6) A palavra VESTIBULAR foi cifrada utilizando uma função cuja inversa é $f^{-1}(x) = \frac{x-4}{2}$. Qual a função cifradora utilizada, e qual a mensagem?
Após a alteração
3) Cifre a palavra C R I P T O G R A F I A, utilizando a função cifradora $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = 3x + 1$. 4) A mensagem T M A C A M L Q C E S G S foi cifrada a partir da função cifradora $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x - 2$. Você seria capaz de descobrir a mensagem original? 5) A palavra V E S T I B U L A R foi cifrada utilizando uma função cifradora $f: \mathbb{Z} \to \mathbb{Z}$ cuja inversa é $f^{-1}(x) = \frac{x-4}{2}$. Qual a função cifradora utilizada, e qual a mensagem?

Fonte: Elaboração própria.

Com isso, os *slides* (APÊNDICE Y) utilizados para auxiliar na atividade de investigação também sofreram alterações para se adequarem a essas mudanças.

Dentre as questões apresentadas na atividade de verificação (APÊNDICE Z), apenas na terceira houve mudança, sendo acrescentado também o conjunto domínio e contradomínio da função dada (Quadro 5).

Quadro 5 – Terceira questão da atividade de verificação

Antes da alteração
3) A palavra MATEMATICA foi cifrada por João utilizando uma chave cuja função decifradora é $f^{-1}(x) = x - 7$. Qual a função cifradora utilizada, e como ficou a mensagem?
Após a alteração
3) A palavra MATEMATICA foi cifrada por João utilizando uma chave cuja função decifradora $f: \mathbb{Z} \to \mathbb{Z}$ é definida por $f^{-1}(x) = x - 7$. Qual a função cifradora utilizada, e como ficou a mensagem?

Fonte: Elaboração própria.

No questionário final (APÊNDICE AA), algumas frases que deveriam ser avaliadas segundo a escala de Likert foram adaptadas com redução no número de afirmações (Quadro 6) após considerações de uma professora que participou do teste exploratório.

Quadro 6 – Afirmações apresentadas no questionário final

Frases antes da alteração	Frases após a alteração
Foi interessante.	Foi interessante.
Agregou novo conhecimento.	Agregou novo conhecimento.
Apresentou relação com conteúdos Matemáticos.	Apresentou relação com conteúdos Matemáticos.
Apresentou linguagem clara.	Foi apresentado de forma clara.
Foi apresentado de maneira atraente.	Foi apresentado de forma atraente.
Foi um estudo diferenciado.	Foi um estudo diferenciado.
Possibilitou a percepção deste tema no cotidiano.	Contribuiu para o estudo da função inversa de uma função afim.
Contribuiu no estudo de função afim.	Tornou o estudo da função inversa mais significativo com aplicação no cotidiano.
Contribuiu no estudo de função inversa da função afim.	Seria importante de ser abordado em sala de aula.
Tornou o estudo de função inversa mais significativo.	
Permitiu estabelecer relação do tema com a função afim e sua inversa.	
Seria interessante abordar esse tema em sala de aula.	

Fonte: Elaboração própria.

Outra alteração que ocorreu no questionário final foi no enunciado da terceira pergunta (Quadro 7). Ao invés de relatarem os pontos positivos e negativos, é solicitado que os alunos avaliem o trabalho.

Quadro 7 – Terceira pergunta do questionário final

Antes da alteração
3- Acerca desse estudo, comente pontos positivos e negativos.
Após a alteração
3- Faça uma avaliação sobre o trabalho.

Fonte: Elaboração própria.

3.3 Experimentação

Para a experimentação da sequência didática na turma regular, foi realizada a escolha de uma turma de 1ª série de uma escola estadual do município de Campos dos Goytacazes. A escolha deu-se pelo fato de que esta turma havia acabado de estudar função afim e sua inversa,

visto que este trabalho objetiva averiguar as possíveis contribuições da Criptografia no estudo destes temas.

A aplicação ocorreu em três encontros, nas aulas de Matemática cedidas pela professora regente da turma. O primeiro encontro durou duas horas-aula, já o segundo e terceiro tiveram duração de três horas-aula, totalizando oito horas-aula.

No primeiro encontro, estiveram presentes 14 alunos, no segundo 12 e no terceiro, 13. Porém, apenas 11 estiveram presentes em todos os encontros, então, apenas esses serão considerados na análise de dados. Os mesmos foram denominados A, B, C, ..., K e essa nomenclatura foi adotada para toda a análise de dados, de modo que o aluno A, por exemplo, será sempre o mesmo em todos os momentos.

Será denominado L um aluno que foi destaque nesse trabalho, este é citado ao longo da experimentação, porém como não participou de todos os encontros, suas respostas não serão computadas nos dados.

3.3.1 Primeiro Encontro: 17/05/2017

Inicialmente, os pesquisadores se apresentaram para a turma e esclareceram o motivo de sua presença ali. Informaram a necessidade da participação de toda a turma em todos os encontros. Em seguida, foram entregues aos alunos o questionário inicial e a atividade de sondagem, para que fizessem individualmente utilizando seus conhecimentos sobre os temas função afim e função inversa (Figura 55).

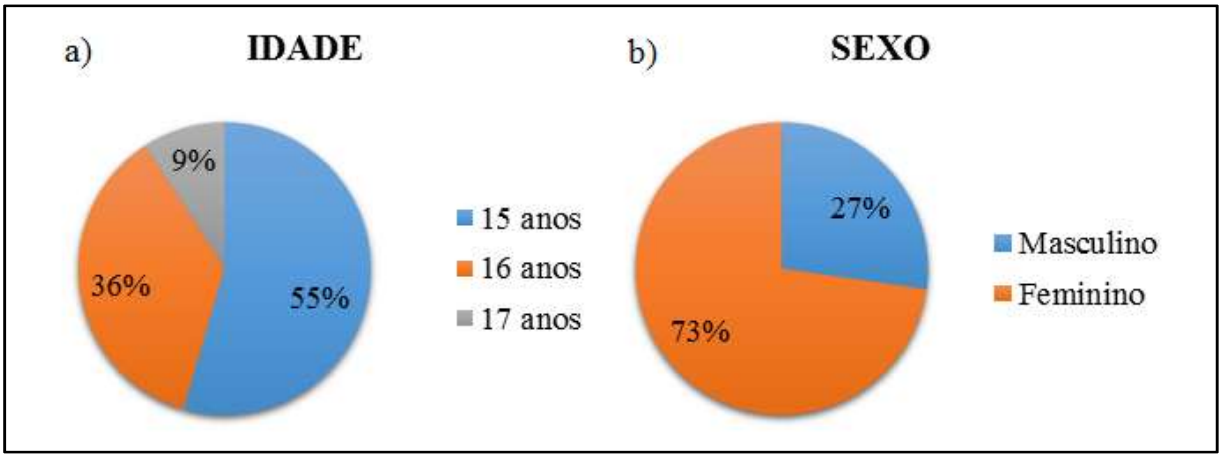
Figura 55 – Aplicação do questionário inicial e da atividade de sondagem

Fonte: Protocolo de pesquisa.

A priori, alguns alunos demonstraram resistência, como no caso do aluno L que devolveu as atividades em branco e se retirou da sala. Após um segundo diálogo com a turma, no qual foi esclarecido que os resultados não seriam para avaliá-los e sim para ajudar a pesquisa, os alunos resistentes decidiram colaborar.

A partir do questionário inicial, pode-se perceber que a pesquisa estava sendo realizada com adolescentes com menos de 18 anos (Gráfico 2 – a), em sua maioria do gênero feminino (Gráfico 2 – b) e que cursaram o ensino fundamental na rede pública.

Gráfico 2 – Idade e sexo dos alunos



Fonte: Elaboração própria.

Em relação ao interesse pela disciplina Matemática, seis afirmaram ter, enquanto cinco afirmaram não ter. Alguns que responderam afirmativamente, comentaram sobre a necessidade da Matemática em algumas profissões (Quadro 8).

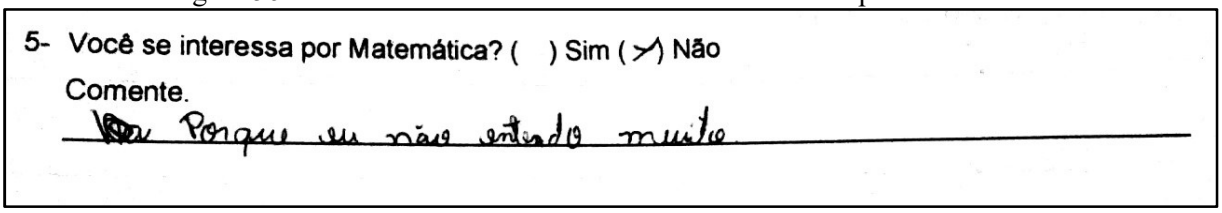
Quadro 8 – Comentários de alunos que afirmaram interesse por Matemática

Comentário do aluno A
5- Você se interessa por Matemática? (X) Sim ( ) Não Comente. Sim. porque futuramente vou exercer a profissão de engenheira civil, então me interesso por essa matéria.
Comentário do aluno B
5- Você se interessa por Matemática? (X) Sim ( ) Não Comente. Sim me interesso pela matemática porque ajuda muito nas coisas principalmente pra quem quer fazer engenharia ou arquitetura.

Fonte: Protocolo de pesquisa.

Os alunos que afirmaram não se interessar por Matemática, declararam que consideram a disciplina chata e de difícil compreensão. Um exemplo é o comentário do aluno C (Figura 56).

Figura 56 – Comentário do aluno C sobre seu desinteresse pela Matemática

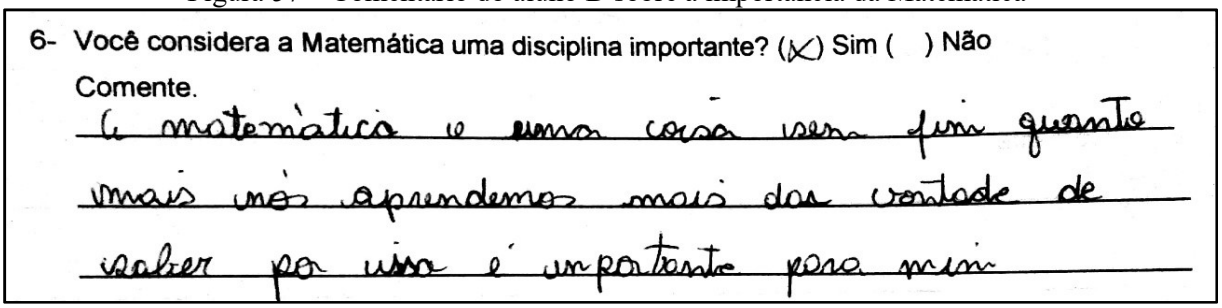


Fonte: Protocolo de pesquisa.

Tais comentários reforçam uma ideia já apresentada no aporte teórico desta pesquisa, que é falta de interesse do aluno em aprender Matemática, ocasionada pela monotonia das aulas, pela falta de relação com o cotidiano e pela falta de desafios, como afirmam Kipper, Ramires e Roos (2006).

Já na sexta pergunta, todos os alunos assinalaram que sim ao serem questionados sobre a importância da disciplina Matemática, destacando a sua utilização no dia a dia. Assim como relatam Bretas e Ferreira (2007), na pesquisa realizada por estes autores constatou-se que os alunos consideram a Matemática como uma ferramenta benéfica nas atividades corriqueiras. O comentário do aluno D (Figura 57) chamou a atenção dos pesquisadores por considerar o estudo da Matemática interessante, ao contrário do que muitos alunos pensam.

Figura 57 – Comentário do aluno D sobre a importância da Matemática



Fonte: Protocolo de pesquisa.

Neste sentido, Ferreira (1998) afirma que:

> Apesar de parecer existir um certo consenso entre a importância da Matemática e à existência de diferentes características desta disciplina em relação à demais, esse consenso parece desaparecer na questão relativa à facilidade/dificuldade de aprender (FERREIRA, 1998 p.118).

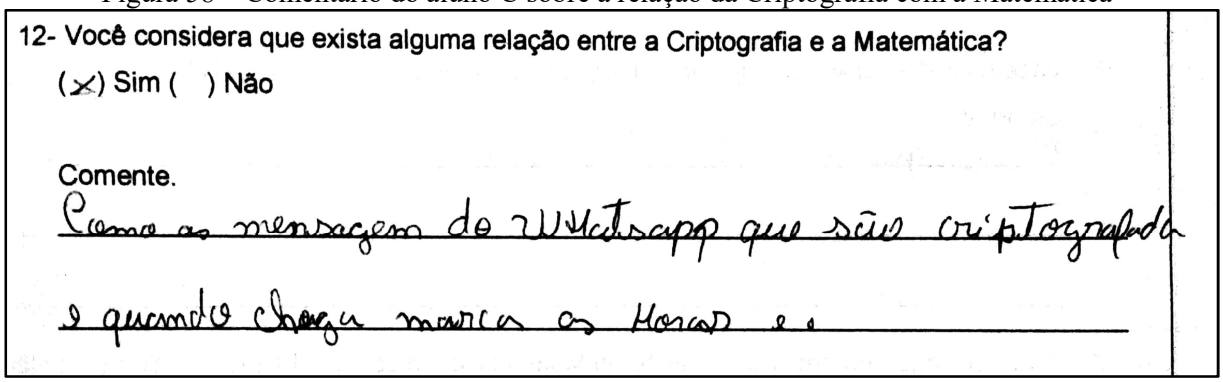
Ao serem questionados sobre a percepção da utilização da Matemática em seu cotidiano, apenas 2 alunos assinalaram que não percebem, enquanto os demais assinalaram que sim e apresentaram como exemplo o uso do dinheiro, horário de entrada na escola, compras, entre outros.

A respeito do estudo de função afim, o aluno E admitiu não ter estudado, apesar desse conteúdo já ter sido trabalhado nessa turma. Com relação ao estudo da função inversa, os 11

alunos afirmaram ter estudado, porém nove indicaram não ter visto aplicação do tema, e dois deixaram em branco. Pode-se ressaltar que alguns alunos apresentaram dificuldade em entender o significado da palavra aplicação, visto que alguns exemplificaram a lei de formação da função como um tipo de aplicação. Após um breve esclarecimento por parte dos pesquisadores, os alunos que haviam assinalado ter visto uma aplicação, alteraram sua resposta.

Sobre o tema Criptografia, quatro alunos comentaram já terem ouvido falar e indicaram sua presença no aplicativo *WhatsApp*. E sobre a existência da relação entre a Criptografia e a Matemática, três consideram que não, quatro deixaram em branco e quatro consideram que sim. Estes últimos, porém, associaram a Matemática ao horário das mensagens recebidas e enviadas no aplicativo que utiliza a Criptografia (Figura 58).

Figura 58 – Comentário do aluno C sobre a relação da Criptografia com a Matemática


12- Você considera que exista alguma relação entre a Criptografia e a Matemática?
(x) Sim ( ) Não

Comente.
Como as mensagem do Whatsapp que são criptografada
e quando chega marca os Horas e e

Fonte: Protocolo de pesquisa.

Na Atividade de Sondagem, cujo objetivo foi captar os conhecimentos dos alunos sobre a função afim e sua inversa, pode-se notar que os alunos confundem com frequência em qual variável devem substituir o valor dado no enunciado. Vale ressaltar ainda que os alunos alegaram não conhecer a notação $f(x)$, o que pode ter influenciado nas respostas incorretas das questões dois e cinco, conforme apresentado na tabela 5. Para o entendimento de tais questões, os pesquisadores esclareceram que $f(x) = y$ e que quando o enunciado pedisse $f(3)$, por exemplo, bastava atribuir à variável x o valor 3.

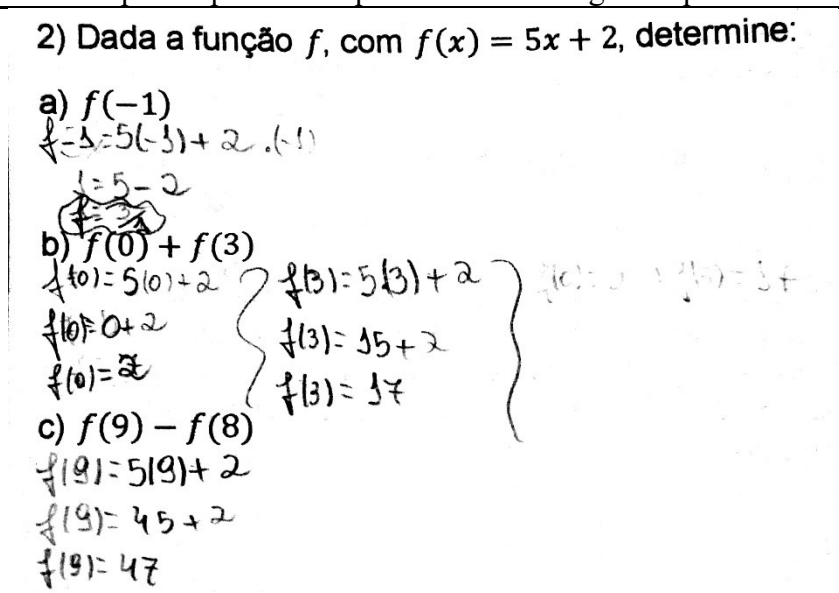
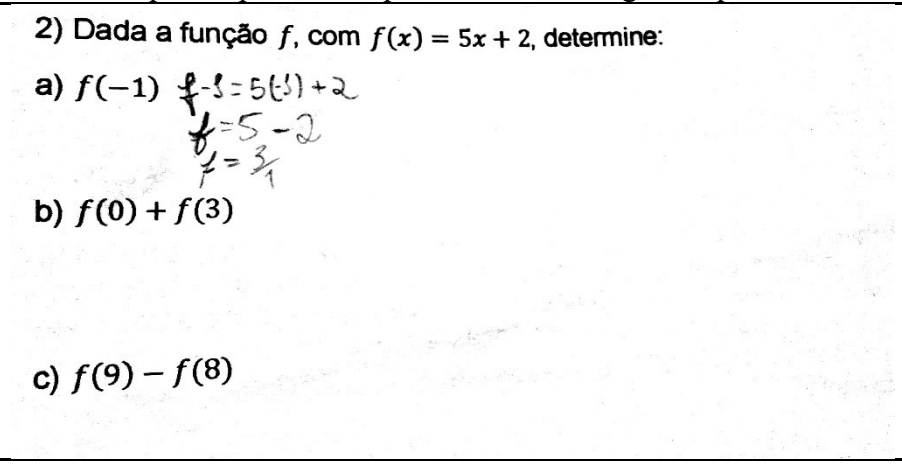
Tabela 5 – Respostas obtidas na atividade de sondagem da experimentação

	Acerto	**Erro**	**Resposta Parcial**	**Em Branco**
1ª Questão – letra a	11	0	0	0
1ª Questão – letra b	11	0	0	0
2ª Questão – letra a	8	3	0	0
2ª Questão – letra b	9	0	1	1
2ª Questão – letra c	9	0	1	1
3ª Questão	11	0	0	0
4ª Questão – letra a	11	0	0	0
4ª Questão – letra b	11	0	0	0
5ª Questão – letra a	11	0	0	0
5ª Questão – letra b	10	1	0	0

Fonte: Elaboração própria.

O aluno F errou a letra *a* da segunda questão, e deixou as letras *b* e *c* parcialmente respondidas. Já o aluno G errou a letra *a* da segunda questão, e deixou em branco as letras *b* e *c* (Quadro 9).

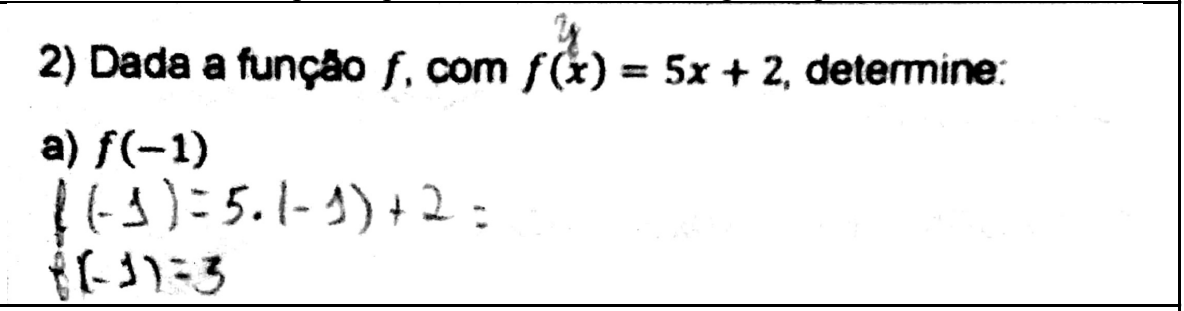
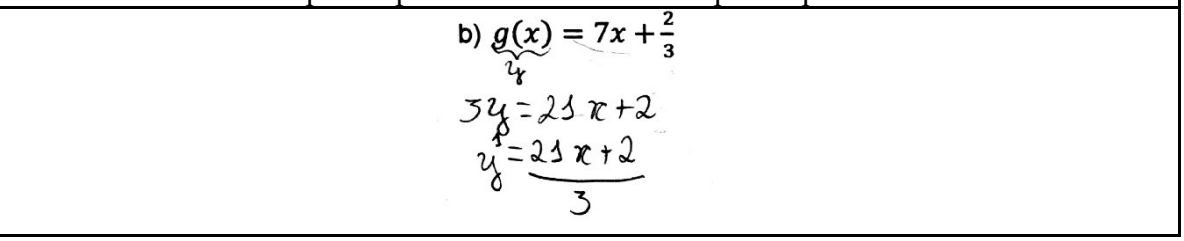
Quadro 9 – Respostas dos alunos F e G na atividade de sondagem

Resposta apresentada pelo aluno F na segunda questão

Resposta apresentada pelo aluno G na segunda questão


Fonte: Protocolo de pesquisa.

O aluno E, que tinha afirmado não ter estudado função afim, errou a letra *a* da segunda questão e a letra *b* da quinta questão (Quadro 10).

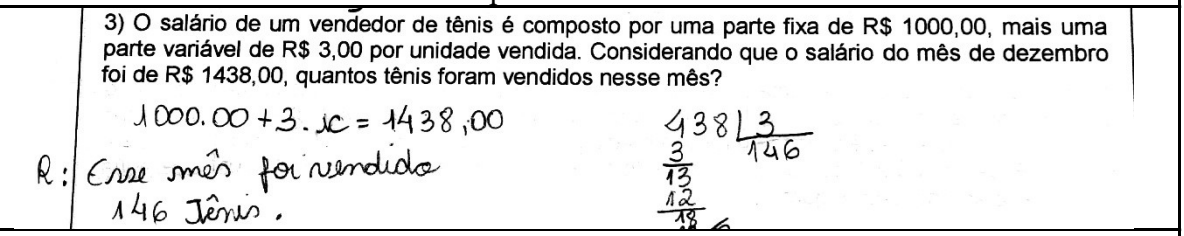
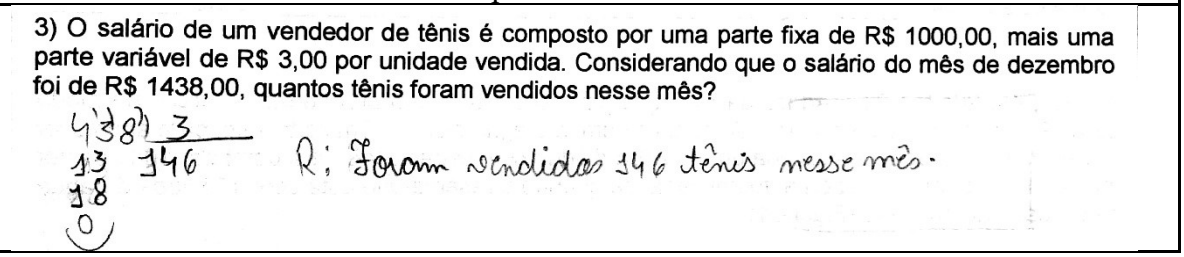
Quadro 10 – Respostas do aluno E na atividade de sondagem

Resposta apresentada na letra *a* da segunda questão

Resposta apresentada na letra *b* da quinta questão


Fonte: Protocolo de pesquisa.

Na questão três, alguns alunos escreveram a lei de formação da função e resolveram o problema conforme esperado pelos pesquisadores, enquanto outros subtraíram a parte fixa do salário e depois dividiram pela taxa mensal para encontrar o valor solicitado, sem escrever a lei de formação da função. O quadro a seguir expõe resoluções que exemplificam os casos mencionados acima, respectivamente (Quadro 11).

Quadro 11 – Respostas na terceira questão da atividade de sondagem

Resposta do aluno D

Resposta do aluno E


Fonte: Protocolo de pesquisa.

3.3.2 Segundo Encontro: 22/05/2017

Para o segundo encontro, foi solicitada à direção uma sala de aula com baixa iluminação que favorecesse a projeção do *datashow*, pois como a sequência didática dispunha de ferramentas como vídeos e *slides*, era de suma importância imagem e som de boa qualidade. Pela quantidade de material necessário para a aplicação das atividades, foi preciso que os pesquisadores estivessem com antecedência no local e que os alunos se deslocassem até essa outra sala mais reservada.

O segundo encontro começou com a fala dos alunos a respeito do que já ouviram falar sobre a Criptografia, a partir do questionamento feito pelos pesquisadores. Os alunos indicaram a presença deste tema no *Facebook* e *WhatsApp*, e os pesquisadores complementaram essas respostas apresentando outros mecanismos que utilizam a Criptografia.

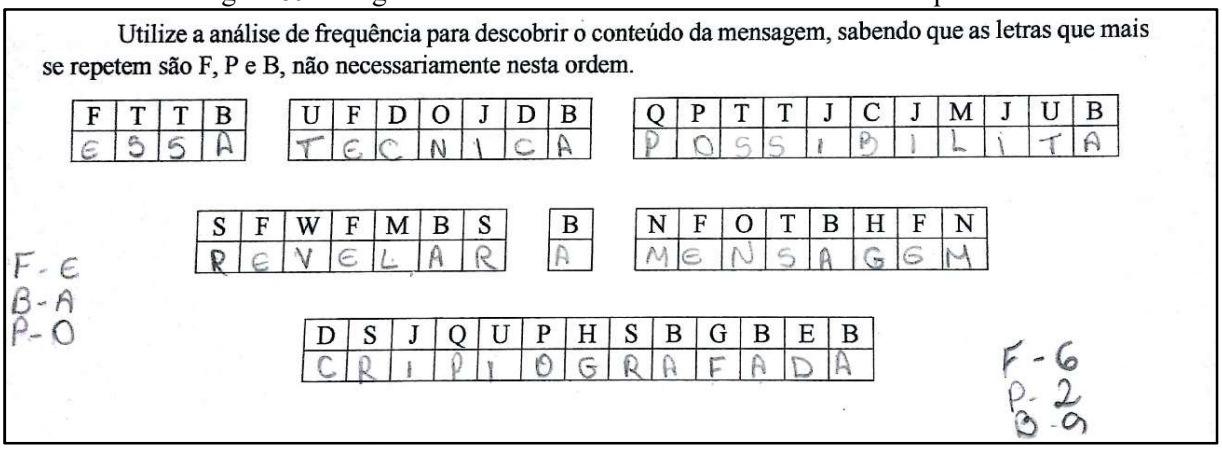
Em seguida, iniciou-se a apresentação da parte histórica da Criptografia, possibilitando assim que os alunos conhecessem um pouco sobre o tema que seria trabalhado.

Nesse momento da aula, os alunos permaneceram atentos durante toda explicação. Embora demostrassem pouca interação inicialmente, aos poucos foram participando ativamente das atividades. Pode-se ressaltar que os pesquisadores auxiliaram os alunos durante a realização das atividades propostas, nos momentos que foram necessários.

Na atividade da cifra de César, houve um equívoco na utilização do disco. Alguns alunos ao invés de mover o disco menor, deslocaram o disco maior. Os pesquisadores analisaram as respostas considerando a interpretação do aluno. Apenas o aluno D cifrou corretamente a mensagem, os demais erraram de uma a três letras, o que é aceitável já que foi o primeiro contato deles com a cifragem de mensagens.

Na atividade da análise de frequência, a maioria acertou e alguns destes apresentaram registro de contagem das letras (Figura 59).

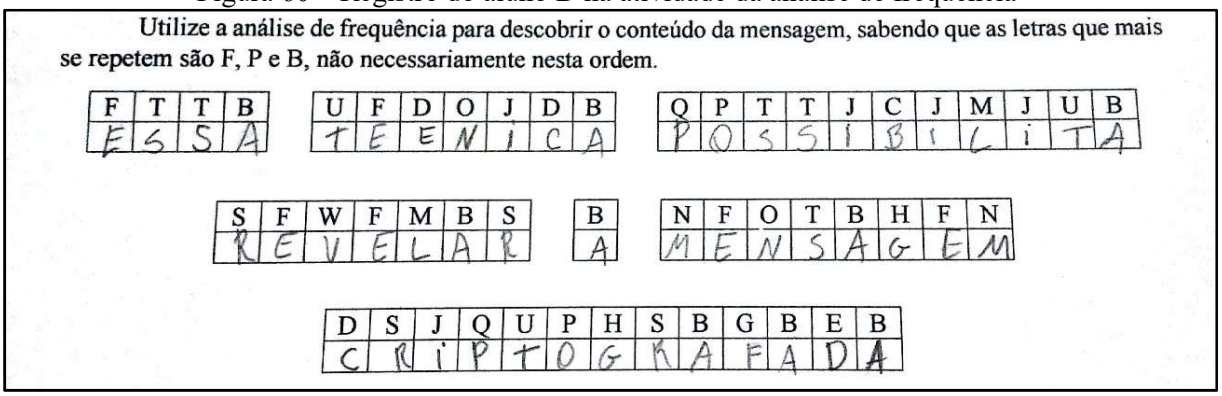
Figura 59 – Registro do aluno A na atividade da análise de frequência



Fonte: Protocolo de pesquisa.

Dois alunos apresentaram como resposta, uma mensagem incoerente. O aluno H apresentou a palavra “PESSIBILITA”, e o aluno D, a palavra “TEENICA” (Figura 60).

Figura 60 – Registro do aluno D na atividade da análise de frequência



Fonte: Protocolo de pesquisa.

Na atividade da cifra de Vigenère, os alunos deveriam encontrar como resposta a mensagem “TUDO E POSSIVEL”, porém três alunos cometeram uma falha na decifragem de uma letra.

Com relação ao tempo disponibilizado para resolução das atividades individuais, apenas a última atividade (cifra de Vigenère) demandou um tempo maior. O aluno D terminou de resolver esta atividade com os pesquisadores durante o intervalo da aula, que ocorreu neste momento.

Após o intervalo, foi apresentado o uso da Criptografia na Segunda Guerra Mundial, nesse momento um aluno comentou a utilização do código Morse[30]. Apesar desse código aparecer no trecho do filme “O Jogo de Imitação” que foi apresentado à turma (Figura 61), não era do interesse dos pesquisadores detalhá-lo. Porém, devido a consideração do aluno, os

[30] O código Morse traduz cada letra do alfabeto numa série de pontos e traços (SINGH, 2001, p. 79).

pesquisadores comentaram que este código é utilizado para transmissão de mensagens, ao invés da ocultação, como é o caso da Criptografia (SINGH, 2001).

Figura 61 – Apresentação do trecho do filme “O Jogo de Imitação”

Fonte: Protocolo de pesquisa.

Em seguida, foi apresentado aos alunos a evolução da Criptografia até os dias atuais e sua importância na garantia da comunicação sigilosa em mecanismos que estes utilizam, como por exemplo, as redes sociais.

No momento da realização das atividades finais (Figura 62), os alunos foram divididos em 3 grupos com 4 alunos cada, denominados Grupo 1, Grupo 2, e Grupo 3.

Figura 62 – Alunos realizando as atividades em grupo

Fonte: Protocolo de pesquisa.

Na atividade da esteganografia, apenas um grupo não apresentou a sequência correta das faces (Figura 63).

Figura 63 – Sequência de faces incorretas apresentada pelo Grupo 1

Fonte: Protocolo de pesquisa.

Na atividade do citale espartano, todos os grupos apresentaram respostas incoerentes (Quadro 12).

Quadro 12 – Respostas apresentadas pelos grupos na atividade do citale espartano

Resposta do Grupo 1
Para trunformar (Verde) a criptografia utilizo mensagem em códigos.
Resposta do Grupo 2
A Criptografia utiliza metodos Para transforma uma mensagem
Resposta do Grupo 3
mensagem em um código APICTOGRAFIA UTILIZA METADOS PARA NOS TRANSFORMA

Fonte: Protocolo de pesquisa.

Em seguida, foi realizada a última atividade, representando o teste de força bruta, momento de grande expectativa dos grupos para testar as chaves acumuladas durante a aula (Figura 64). O Grupo 2 conseguiu abrir o cadeado com a chave de número 6.

Figura 64 – Teste de abertura do cadeado

Fonte: Protocolo de pesquisa.

Destaca-se o interesse e a empolgação dos alunos durante a realização das atividades, principalmente quanto a conquista das chaves. Ressalta-se a participação do aluno L, que, ao conquistar a chave colou-a em sua testa expondo seu entusiasmo, embora tenha se mostrado relutante a princípio.

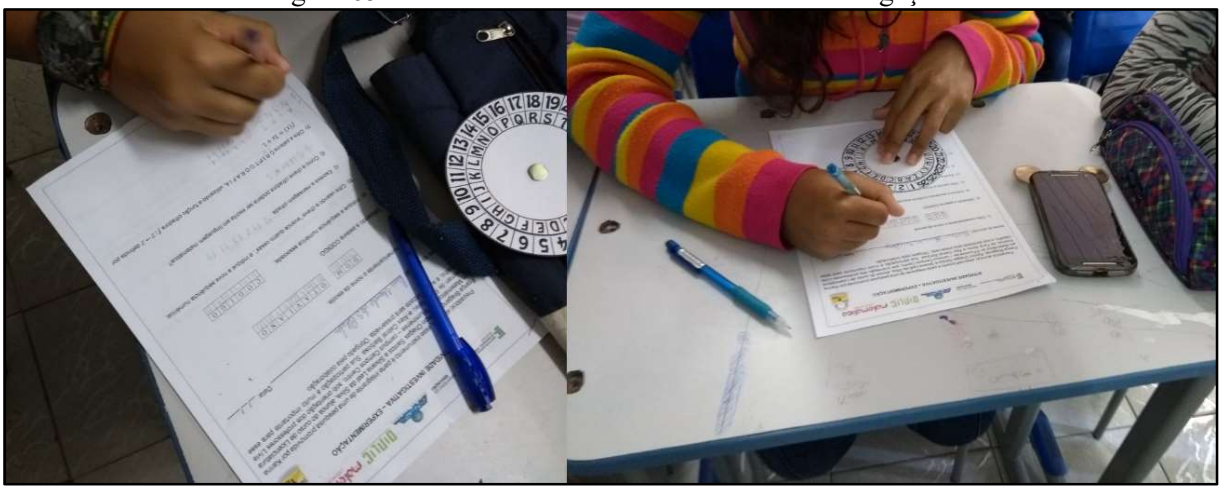
Ao finalizar a aula, os pesquisadores concluíram, a partir da interação, e motivação dos alunos e dos resultados obtidos, que a inserção da contextualização de um tema matemático desperta o interesse do aluno para a aprendizagem. Além disso, os conhecimentos adquiridos contribuíram para o próximo encontro, em que objetiva-se relacionar a Criptografia à função afim e sua inversa.

3.3.3 Terceiro Encontro: 23/05/2017

Dando continuidade ao encontro anterior, os pesquisadores retornaram à turma e perceberam grande animação por parte dos alunos. Os mesmos relataram terem criado um grupo no *WhatsApp*, afim de conversarem utilizando códigos.

Neste encontro, foi entregue uma apostila, a atividade de investigação, com questões que relacionavam a Criptografia com a Matemática. Para esse primeiro contato, os pesquisadores auxiliaram nas resoluções (Figura 65), solicitando a participação dos alunos a todo momento.

Figura 65 – Alunos realizando a atividade de investigação



Fonte: Protocolo de pesquisa.

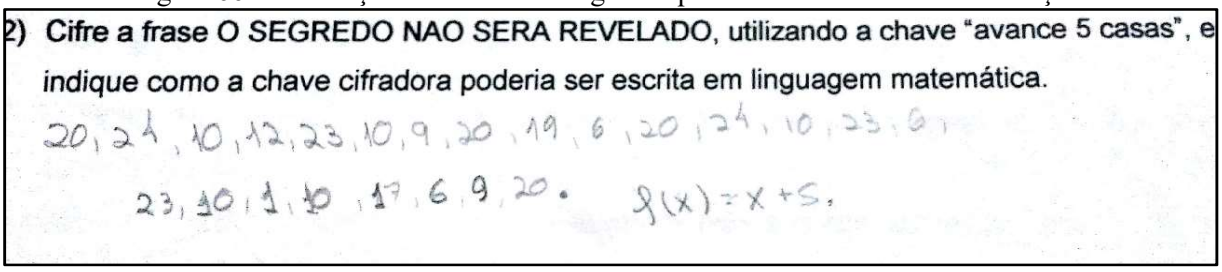
No encontro anterior, os alunos foram capazes de estabelecer a compreensão sobre o fato de que a decifragem de uma mensagem envolve o processo inverso da cifragem da mesma. Com isso, ao aplicar esta atividade de investigação, pode-se perceber que os alunos não apresentaram dificuldades em relacionar a cifragem e decifragem com os conceitos de função afim e sua inversa, respectivamente.

Ao serem questionados sobre a representação matemática que envolvia a chave solicitada na questão dois, item d, a maioria conseguiu associá-la a função afim $f(x) = x + 4$. E, para provocar no aluno a percepção sobre o fato de que a função decifradora é obtida a partir da inversa da função cifradora, foi indagado, pelos pesquisadores, qual seria o processo a ser realizado para se obter a mensagem original. Nesse momento, alguns alunos responderam que neste caso era necessário recuar quatro casas, isto é, retirar quatro unidades, que remete a função inversa $f^{-1}(x) = x - 4$.

A última questão da atividade de investigação, como descrito anteriormente, foi realizada em grupo. Esta questão foi desafiadora para os alunos, por se tratar de uma questão adaptada da OBMEP que envolvia o uso do raciocínio lógico. Os alunos apresentaram dificuldades em sua resolução, e embora tenha ultrapassado o tempo destinado, os pesquisadores decidiram estender este prazo, visto que os alunos demonstraram motivação e interesse em resolvê-la. As respostas dessa atividade foram registradas na ficha em formato de cadeado e entregue aos pesquisadores para finalizar a pontuação da gincana.

Em seguida, foi entregue aos alunos a atividade de verificação. Todos os alunos acertaram a primeira e a segunda questão desta atividade, apesar de apresentarem apenas a mensagem cifrada numericamente na questão dois (Figura 66).

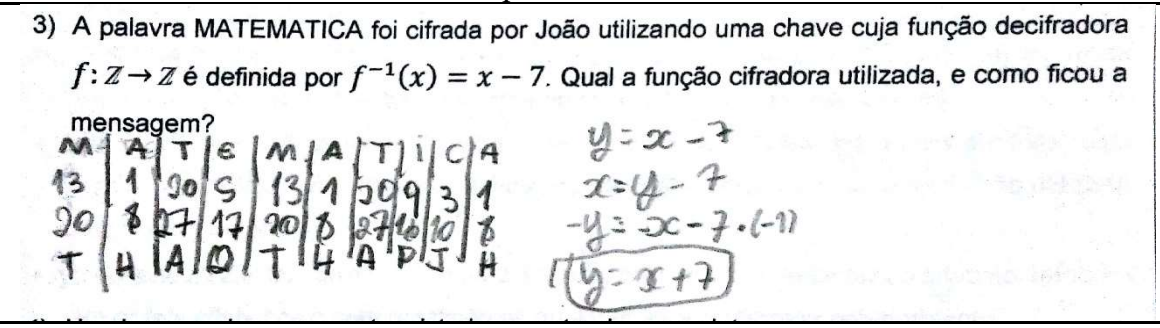
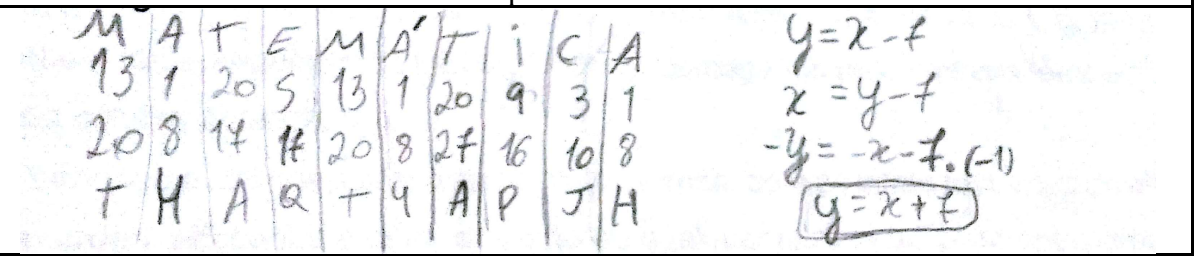
Figura 66 – Resolução do aluno I na segunda questão da atividade de verificação



Fonte: Protocolo de pesquisa.

Já na terceira questão, dois alunos se equivocaram na cifragem da letra *e*, que foi cifrada pela letra Q ao invés de ser cifrada pela letra L (Quadro 13).

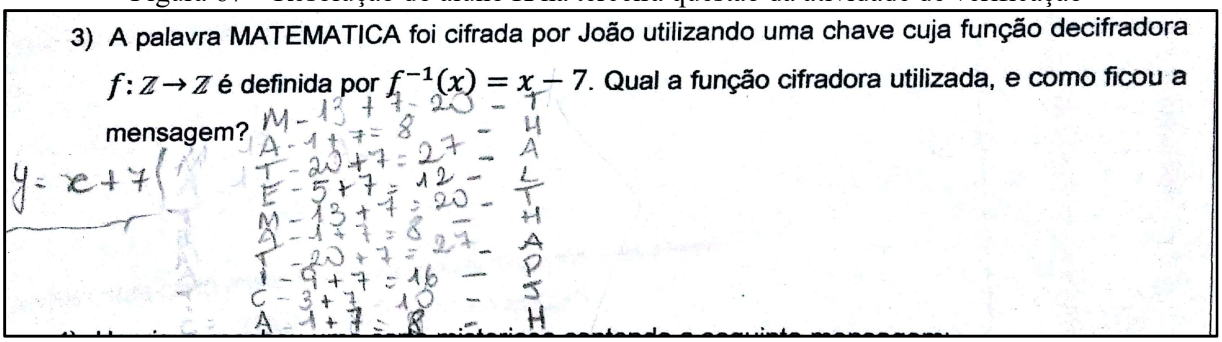
Quadro 13 – Respostas incorretas na terceira questão da atividade de verificação

Resposta do aluno G

Resposta do aluno J


Fonte: Protocolo de pesquisa.

Os demais alunos responderam como o esperado, associando as letras corretamente, assim como o aluno K (Figura 67).

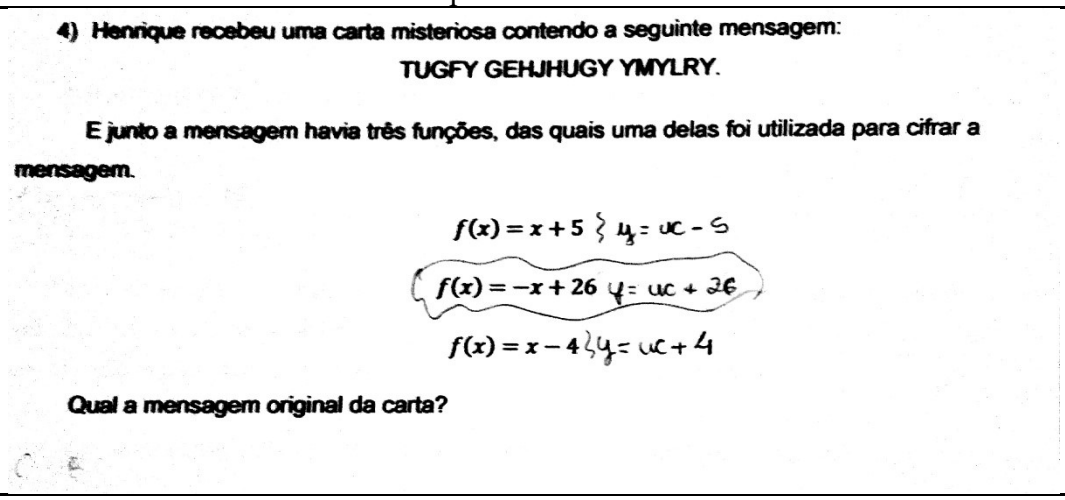
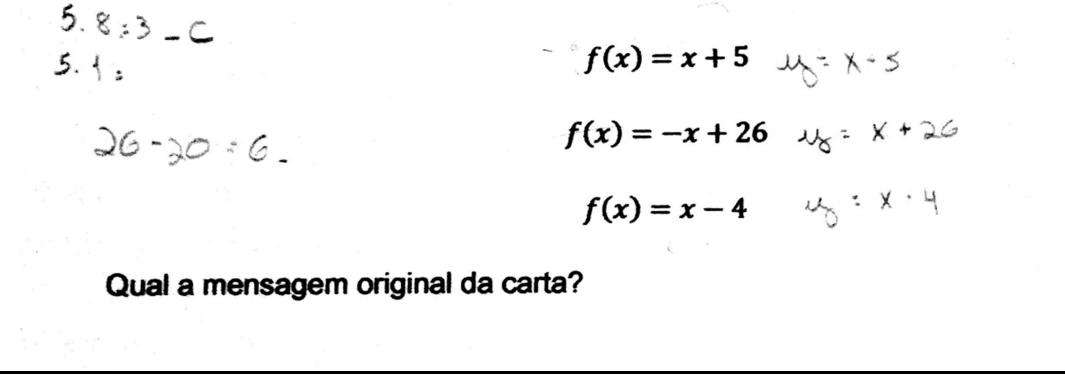
Figura 67 – Resolução do aluno K na terceira questão da atividade de verificação



Fonte: Protocolo de pesquisa.

Por conta do atraso na resolução da questão da OBMEP e a proximidade do término do horário da aula, os pesquisadores comunicaram aos alunos que não havia a necessidade de resolverem a quarta questão. Porém, a maioria dos alunos conseguiu resolvê-la. Apenas um aluno não respondeu e dois deixaram a questão parcialmente respondida, indicando apenas as funções inversas das funções dadas (Quadro 14).

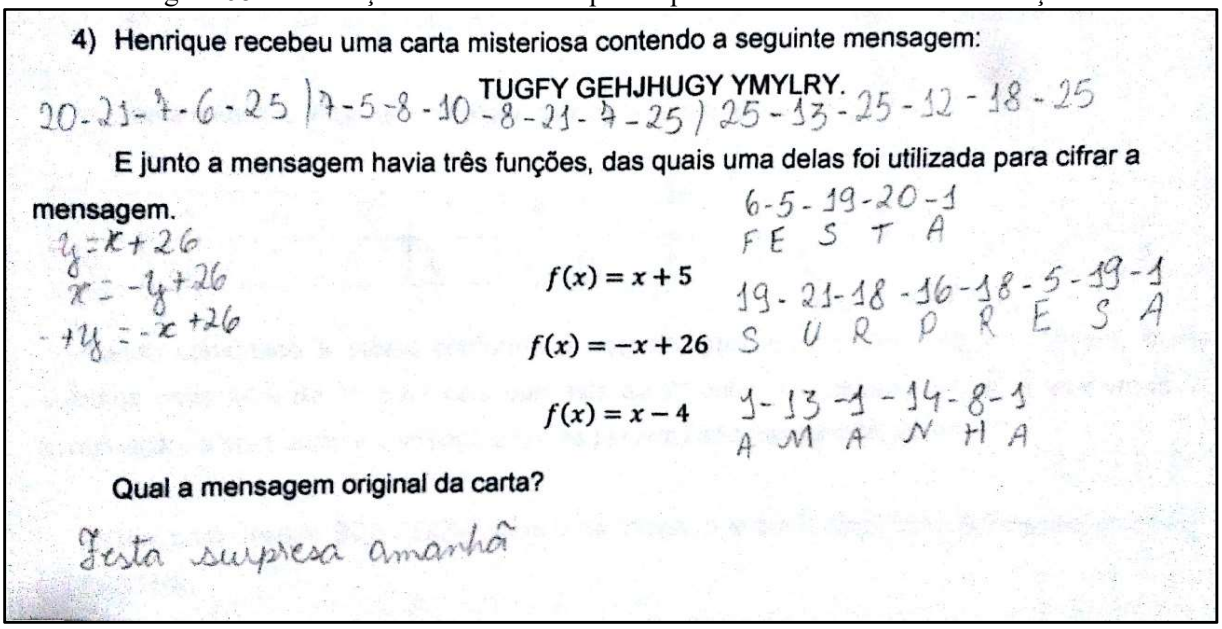
Quadro 14 – Respostas incompletas na quarta questão da atividade de verificação

Resposta do aluno D

Resposta do aluno I


Fonte: Protocolo de pesquisa.

Dentre as respostas corretas, destaca-se a do aluno E (Figura 68) que no questionário inicial relatou não ter estudado função afim e errou duas questões na atividade de sondagem. O mesmo apresentou a resposta de forma coerente e organizada, sinalizando uma melhora no desempenho desse aluno.

Figura 68 – Resolução do aluno E na quarta questão da atividade de verificação



Fonte: Protocolo de pesquisa.

O questionário final foi aplicado ao final do encontro, e em sua análise constata-se, de modo geral, uma avaliação positiva por parte dos alunos quanto à escolha do tema, ao desenvolvimento da aula e à atuação dos pesquisadores. A tabela 6 a seguir apresenta dados coletados a partir do questionário final.

Tabela 6 – Respostas obtidas no questionário final

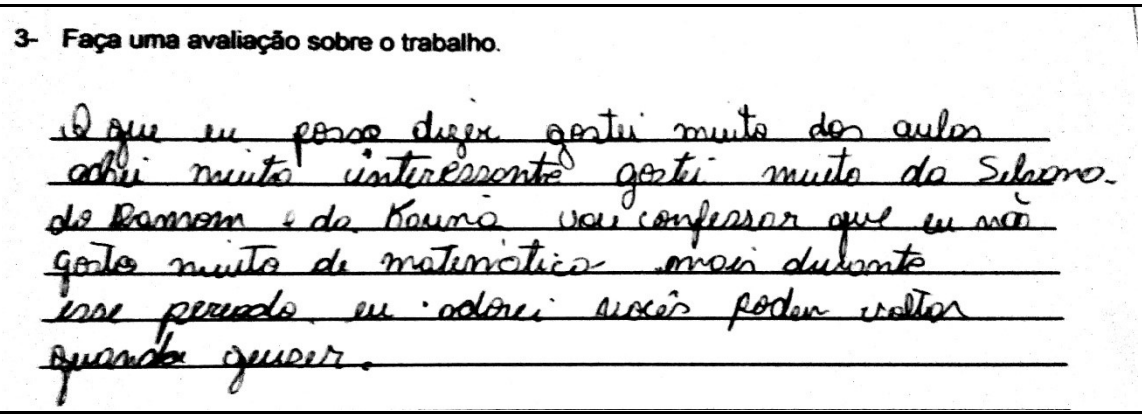
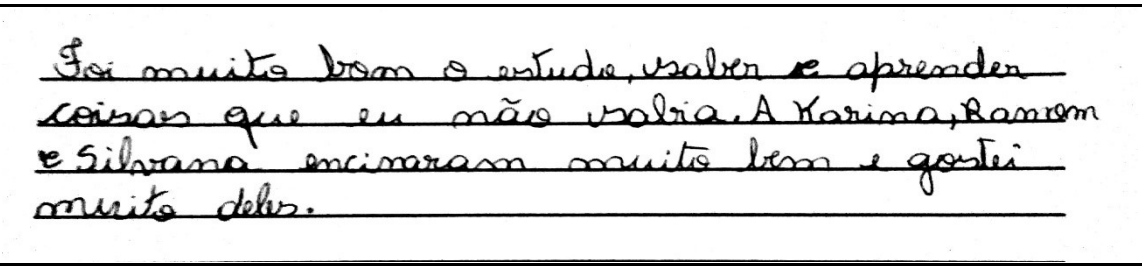
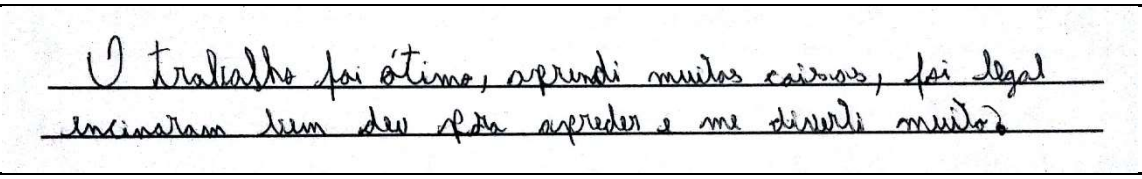
	D	DP	NC/ND	CP	C
Foi interessante.	0	0	0	0	10
Agregou novo conhecimento.	0	0	0	0	11
Apresentou relação com conteúdos Matemáticos.	0	0	0	0	11
Foi apresentado de forma clara.	0	0	0	2	9
Foi apresentado de forma atraente.	0	0	0	0	11
Foi um estudo diferenciado.	0	0	0	0	11
Contribuiu para o estudo da função inversa de uma função afim.	0	0	0	0	11
Tornou o estudo da função inversa mais significativo com aplicação no cotidiano.	0	0	0	0	11
Seria interessante abordar esse tema em sala de aula.	0	0	1	2	8

Fonte: Elaboração própria.

Observação: O aluno K não marcou o primeiro item, e o aluno G assinalou NC/ND no último item, porém não justificou.

Na avaliação subjetiva sobre o trabalho, a maioria dos alunos relatou que a aula foi produtiva e que o tema foi apresentado de forma interessante. Segue comentários de três alunos no quadro 15.

Quadro 15 – Comentários relatados no questionário final

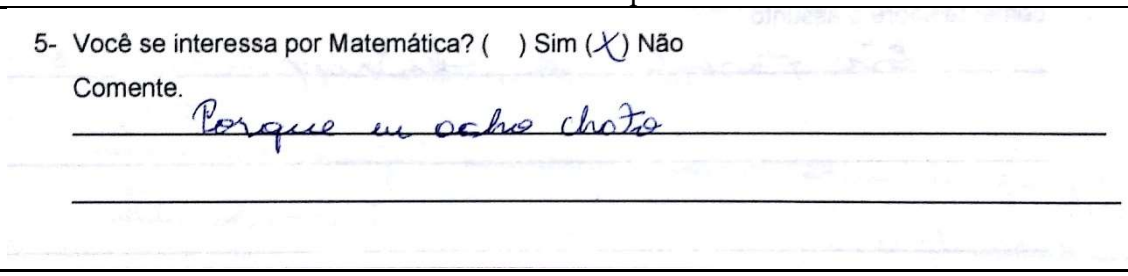
Comentário do aluno D

Comentário do aluno F

Comentário do aluno H


Fonte: Protocolo de pesquisa.

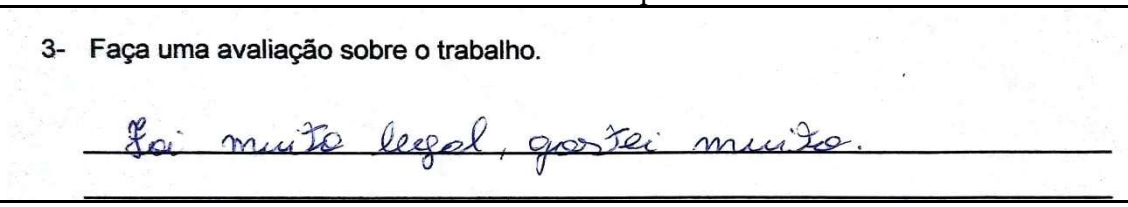
Ao comparar as respostas dos alunos que indicaram não gostar de Matemática no questionário inicial com os seus comentários positivos após o término da aula (Quadro 16), reforça-se a importância da utilização da contextualização como ferramenta no ensino de Matemática. Os pesquisadores avaliam que a utilização da Criptografia na sequência didática apresentada contribuiu para modificar o pensamento de alguns alunos em relação a aula Matemática, tornando-a mais atrativa.

Quadro 16 – Respostas apresentadas por três alunos nos questionários inicial e final

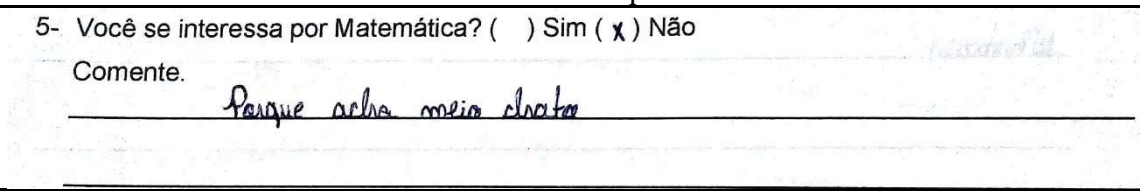
Comentário do aluno J no questionário inicial


5- Você se interessa por Matemática? ( ) Sim (X) Não
Comente.
Porque eu acho chato

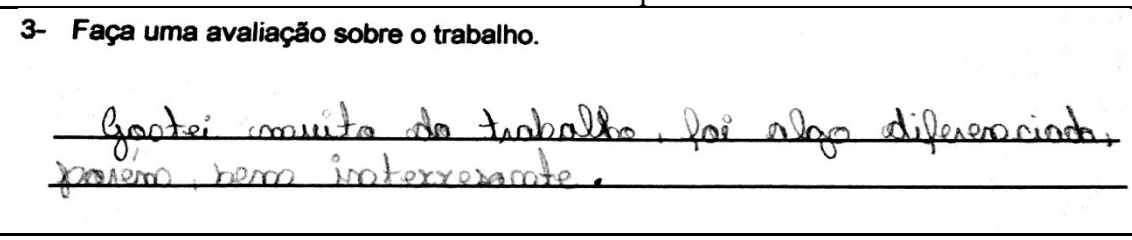
Comentário do aluno J no questionário final


3- Faça uma avaliação sobre o trabalho.
Foi muito legal, gostei muito.

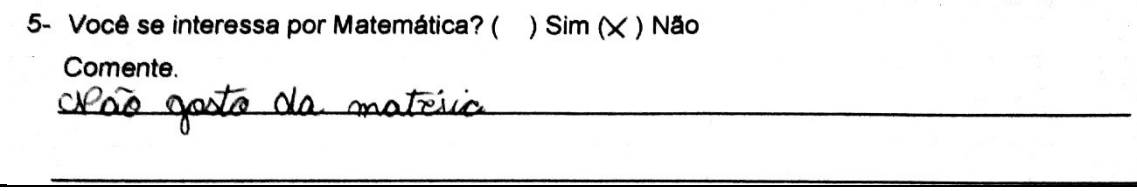
Comentário do aluno I no questionário inicial


5- Você se interessa por Matemática? ( ) Sim (x) Não
Comente.
Porque acha meio chato

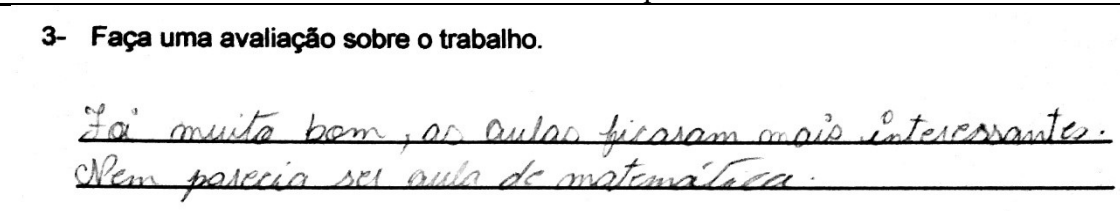
Comentário do aluno I no questionário final


3- Faça uma avaliação sobre o trabalho.
Gostei muito do trabalho, foi algo diferenciado, passeio, bem interessante.

Comentário do aluno E no questionário inicial


5- Você se interessa por Matemática? ( ) Sim (X) Não
Comente.
Não gosto da matéria

Comentário do aluno E no questionário final


3- Faça uma avaliação sobre o trabalho.
Foi muito bom, as aulas ficaram mais interessantes. Nem parecia ser aula de matemática.

Fonte: Protocolo de pesquisa.

Estes comentários reforçam a ideia de que “por meio de atividades contextualizadas, o professor consegue mostrar a naturalidade do conhecimento matemático e que, muitas vezes, o aluno “faz matemática” sem perceber” (PEREIRA, V. 2012).

Os pesquisadores encerraram a aula agradecendo a professora regente da turma e os alunos que participaram da pesquisa. Em seguida premiaram o grupo vencedor da gincana, o Grupo 2. Distribuíram livros da OBMEP que abordam o tema Criptografia e bombons para todos os alunos.

CONSIDERAÇÕES FINAIS

A Criptografia é um tema abrangente e atual, sua história é bem rica e interessante, e estas características serviram de motivação para a realização deste trabalho.

O estudo promovido inicialmente, mostrou como a Matemática está diretamente associada a este tema, ou seja, sua ligação ao sigilo de informações. As pesquisas realizadas apontaram uma variedade de trabalhos que relacionam a Criptografia a diferentes conteúdos matemáticos, o que destaca sua potencialidade no ensino desta disciplina.

A partir disso, foi elaborada uma sequência didática com o intuito de relacionar os temas Criptografia e função afim e sua inversa, de forma atrativa, dinâmica e diversificada.

Esta sequência foi aplicada inicialmente à graduandos em Matemática e convidados, sendo de suma importância para ressaltar os aspectos coerentes com os objetivos traçados e aqueles que necessitavam de modificações.

A experimentação na turma regular proporcionou, de acordo com os resultados obtidos, uma contribuição no processo de ensino e aprendizagem de função afim e sua inversa, o que justifica a escolha da pesquisa do tipo intervenção pedagógica.

A inserção da história da Criptografia foi essencial para oportunizar ao aluno o conhecimento acerca desse tema, além de proporcionar contexto à aula elaborada. Os mecanismos utilizados para isso foram de extrema relevância para a concretização de tais ideias. Dentre eles podemos destacar a utilização de materiais construídos pelos pesquisadores e a gincana realizada.

É importante destacar que, utilizando dos conhecimentos pré-existentes dos alunos, a contextualização proporcionada pelo tema Criptografia despertou motivação e interesse destes, ao perceberem que o processo, aparentemente mecanizado, de determinação da inversa de uma função afim tem sentido e significação.

Sendo assim, a Criptografia se mostrou um material potencialmente significativo e que desperta a curiosidade do aluno e o desejo de aprender. Corroborando com a teoria da Aprendizagem Significativa de Ausubel, houve uma interação entre esse novo conhecimento e os conhecimentos já adquiridos pelos alunos previamente, de modo a se modificarem, contribuindo com o processo de ensino e aprendizagem.

As atividades propostas neste trabalho 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 de função afim e sua inversa, proporcionando significado à sua aprendizagem.

Para estudos futuros, sugere-se a utilização da Criptografia como ferramenta no estudo de outros tipos de funções, tais como a função exponencial e logarítmica; além de enfatizar os conceitos de domínio e do conjunto imagem das funções. A apresentação deste tema também pode contextualizar o ensino de outros conteúdos matemáticos, como análise combinatória, matrizes, entre outros.

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.

Enfim, constatou-se por meio da investigação que a Criptografia contribui para o ensino e aprendizagem de função afim e sua inversa ao contextualizar seu estudo e proporcionar uma aprendizagem significativa.

REFERÊNCIAS

ALVES, Paulo. O que é HTTPS e como ele pode proteger a sua navegação na Internet. **TechTudo,** [s.l.], 20 fev. 2014. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2014/02/o-que-e-https-e-como-ele-pode-proteger-sua-navegacao-na-internet.html>. Acesso em: 24 ago. 2017.

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>. Acesso em: 26 dez. 2016.

BRASIL. **Guia de livros didáticos:** PNLD 2015: Matemática: Ensino Médio. Brasília: Ministério da Educação, Secretaria de Educação Básica, 2014.

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

BRASIL. Secretaria da Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais:** Ensino Médio. Brasília: MEC, 2000.

BRASIL. Tribunal Superior Eleitoral. **Por que a urna eletrônica é segura.** Relator: Rodrigo Carneiro Munhoz Coimbra, [s.d.]. Disponível em: <http://www.tse.jus.br/institucional/escola-judiciaria-eleitoral/revistas-da-eje/artigos/revista-eletronica-eje-n.-6-ano-4/por-que-a-urna-eletronica-e-segura>. Acesso: 24 ago. 2017.

BRETAS, Simone Nazaré Ribeiro; FERREIRA, Ana Cristina. A percepção da Matemática pelos alunos de 8ª série do ensino fundamental de escolas de Cachoeiro do Campo. In: ENCONTRO NACIONAL DE EDUCAÇÃO MATEMÁTICA. 9., 2007, Belo Horizonte. **Anais...** Belo Horizonte, 2007.

COUTINHO, Severino Collier. **Criptografia.** Rio de Janeiro, IMPA, 2014.

CRESWELL, John W. **Projeto de pesquisa:** métodos qualitativo, quantitativo e misto. Tradução de Luciana de Oliveira da rocha. 2. ed. Porto Alegre: Artmed, 2007.

DAMIANI, Magda Floriana. Sobre Pesquisas do Tipo Intervenção. In: ENCONTRO NACIONAL DE DIDÁTICA E PRÁTICAS DE ENSINO, 16., 2012, Campinas. **Anais...** Campinas: UNICAMP, 2012. Disponível em: < http://www.infoteca.inf.br/endipe/smarty/templates/arquivos_template/upload_arquivos/acervo/docs/2345b.pdf>. Acesso em: 26 dez. 2016.

DAMIANI, Magda et al. Discutindo pesquisas do tipo intervenção pedagógica. **Cadernos de Educação.** FaE/PPGE/UFPel. Nº 45. p. 57-67, 2013. Disponível em: <https://periodicos.ufpel.edu.br/ojs2/index.php/caduc/article/view/3822>. Acesso em: 08 set. 2017.

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.

DESLANDES, Suely Ferreira et al (Org.). **Pesquisa social:** teoria, método e criatividade. 21. ed. Petrópolis: Vozes, 2002.

FERREIRA, Ana Cristina. **Desafio de ensinar-aprender Matemática no curso noturno:** Um estudo das crenças de estudantes de uma escola pública de Belo Horizonte. Dissertação (Mestrado em Educação Matemática) – Faculdade de Educação, Universidade Estadual de Campinas, Campinas, 1998. Disponível em: < http://www.educadores.diaadia.pr.gov.br/arquivos/File/2010/artigos_teses/MATEMATICA/Dissertacao_Ferreira.pdf>. Acesso em: 14 set. 2017.

FULGÊNCIO, Caio**.** Jovem desaparecido deixou 'chave' para decifrar livros criptografados, diz família. **G1**, Rio Branco, 05 abr. 2017. Disponível em: <http://g1.globo.com/ac/acre/noticia/jovem-desaparecido-deixou-chave-para-decifrar-livros-criptografados-diz-familia.ghtml>. Acesso em: 13 ago. 2017.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo (Org.). **Métodos de Pesquisa.** Porto Alegre: Editora da UFRGS, 2009.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 6.ed. São Paulo: Atlas, 2012.

JESUS, Adriana Garabini de. **A Motivação para aprender Matemática no 9º ano do Ensino Fundamental:** um estudo do potencial dos materiais manipulativos e da construção de objetos na aprendizagem de área de polígonos e volume de prismas. 2011. Dissertação (Mestrado em Educação Matemática) – Instituto de Ciências Exatas e Biológicas, Universidade Federal de Ouro Preto, Ouro Preto, 2011. Disponível em: <http://www.repositorio.ufop.br/bitstream/123456789/1287/1/EVENTO_Motiva%C3%A7%C3%A3oAlunoAprender.pdf>. Acesso em: 08 set. 2017.

KATO, Danilo Seithi, KAWASAKI, Clarice Sumi. O significado da contextualização no ensino de ciências: análise dos documentos curriculares oficiais e de professores. In: ENCONTRO NACIONAL DE PESQUISA EM EDUCAÇÃO EM CIÊNCIAS, 6., 2007, Florianópolis. **Anais...** Florianópolis, 2007. Disponível em: <www.nutes.ufrj.br/abrapec/vienpec/CR2/p782.pdf>. Acesso em: 08 set. 2017.

KIPPER, Cristine Maria; RAMIRES, Janaína Iochims, ROOS, Liane Teresinha Wendling. Geometria e Natureza: Uma Associação Perfeita para Trabalhar Conceitos Geométricos. In: ENCONTRO GAÚCHO DE EDUCAÇÃO MATEMÁTICA, 9., 2006, Caxias do Sul. **Anais...** Caxias do Sul, 2006. Disponível em: < http://miltonborba.org/CD/Interdisciplinaridade/Encontro_Gaucho_Ed_Matem/cientificos/CC85.pdf >. Acesso em: 14 set. 2017.

LIMA, Elon Lages. Conceituação, Manipulação e Aplicação: Os três componentes do ensino da Matemática. **Revista do Professor de Matemática**, São Paulo: Sociedade Brasileira de Matemática, n. 41, p. 1-6, 1999.

LITOLDO, Beatriz Fernanda. **As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim.** 2016. Dissertação (Mestrado em Educação Matemática) – Instituto de Geociências e Ciências

Exatas, Universidade Estadual Paulista, Rio Claro, 2016. Disponível em: <http://repositorio.unesp.br/bitstream/handle/11449/141470/litoldo_bf_me_rcla.pdf?sequence=3&isAllowed=y>. Acesso em: 26 dez. 2016.

LOUREIRO, Flávio Ornellas. **Tópicos de criptografia para o ensino médio.** 2014. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) - Universidade Estadual do Norte Fluminense Darcy Ribeiro, Campos dos Goytacazes, 2014. Disponível em: <http://www.sbmac.org.br/eventos/cnmac/xxxi_cnmac/PDF/189.pdf http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/1528/2012_01339_FLAVIO_ORNELLAS_LOUREIRO.pdf?sequence=1>. Acesso em: 26 dez. 2016.

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

MICOTTI, Maria Cecília de Oliveira. O ensino e as propostas pedagógicas. In: BICUDO, Maria Aparecida Viggiani (Org.). **Pesquisa em educação matemática:** concepções e perspectivas. São Paulo: Editora UNESP, 1999.

MORAN, José Manuel. **Como ver televisão:** leitura e crítica dos meios de comunicação. São Paulo: Editora Paulinas, 1991.

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.

NUNES, Ana Ignez Belém Lima; SILVEIRA, Rosemary do nascimento. **Psicologia da aprendizagem: processos, teorias e contextos.** 3. ed. Brasília: Liber Livro, 2011.

OLIVEIRA, Fabiane dos Santos. **Lúdico como instrumento facilitador na aprendizagem da educação infantil.** 2010. Monografia (Pós-Graduação em Psicopedagogia Institucional) – Universidade Candido Mendes, Araioses, 2010. Disponível em: < http://www.avm.edu.br/docpdf/monografias_publicadas/posdistancia/35505.pdf>. Acesso em: 02 set. 2017.

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.

PINHEIRO, Filipa Margarida Dias Lima. **CONTEXTUALIZAÇÃO DO SABER:** Formação Inicial dos Professores de 1º e 2º Ciclo do Ensino Básico. 2012. Dissertação (Mestrado em Ciência da Educação) – Instituto de Educação, Universidade de Lisboa. 2012. Disponível em:

<http://repositorio.unesp.br/bitstream/handle/11449/141470/litoldo_bf_me_rcla.pdf?sequence=3&isAllowed=y>. Acesso em: 08 set. 2017.

SANTOS, Anderson Oramisio. Aspectos pedagógicos da aprendizagem significativa de Ausubel em matemática nos primeiros anos de ensino fundamental. In: ENCONTRO MINEIRO DE EDUCAÇÃO MATEMÁTICA, 7., 2015, Minas Gerais. **Anais...** Minas Gerais: Universidade Federal de São João del-Rei, 2015. Disponível em: < http://www.ufjf.br/emem/files/2015/10/ASPECTOS-PEDAG%C3%93GICOS-DA-APRENDIZAGEM-SIGNIFICATIVA-DE-AUSUBEL-EM-MATEM%C3%81TICA-NOS-PRIMEIROS-ANOS-DO-ENSINO-FUNDAMENTAL.pdf>. Acesso em: 08 set. 2017.

SANTOS, José Luiz dos. **A Arte de Cifrar, Criptografar, Esconder e Salvaguardar 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.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/208/2011_00046_JOSE_LUIZ_DOS_SANTOS.pdf?sequence=1>. Acesso em: 26 dez. 2016.

SANTOS, Simone Cardoso dos. **A importância do lúdico no processo de ensino e aprendizagem.** 2010. Monografia (Curso de Pós-Graduação a Distância Especialização Lato-Sensu em Gestão Educacional) – Universidade Federal de Santa Maria, Santa Maria-RS, 2010. Disponível em: < http://repositorio.ufsm.br/bitstream/handle/1/393/Santos_Simone_Cardoso_dos.pdf?sequence=1>. Acesso em: 02 set. 2017.

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.

SIQUEIRA, Josué Rangel de. **A natureza sob um prisma matemático.** 2016. Monografia (Licenciatura em Matemática). Instituto Federal de Educação, Ciência e Tecnologia Fluminense, Campos dos Goytacazes, 2016. Disponível em: <http://licenciaturas.centro.iff.edu.br/cursoslicenciatura/licenciatura-em-matematica/trabalho-de-conclusao-de-curso/2015/a-natureza-sob-um-prisma-matematico/view>. Acesso em: 08 set. 2017.

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

APÊNDICES

APÊNDICE A: Questionário Inicial – Teste Exploratório

QUESTIONÁRIO I – TESTE EXPLORATÓRIO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

1- Nome do aluno(a): _____

2- Sexo: ( ) Masculino ( ) Feminino

3- Idade: _____

4- Cursou o 9º ano do ensino fundamental em: ( ) escola particular ( ) escola pública

5- Você se interessa por Matemática? ( ) Sim ( ) Não
Comente.

_____

_____

_____

6- Você considera a Matemática uma disciplina importante? ( ) Sim ( ) Não
Comente.

_____

_____

_____

7- Você consegue perceber a utilização da Matemática em seu cotidiano? ( ) Sim ( ) Não

7.1 - Caso tenha assinalado "Sim" no item acima, indique um exemplo. _____

_____

8- Você já estudou função afim? ( ) Sim ( ) Não

9- Você já estudou função inversa? ( ) Sim ( ) Não

Caso tenha assinalado "Sim" no item 9, responda o item abaixo.

10- Ao estudar a função inversa, foi apresentada alguma aplicação sobre esse tema?
( ) Sim ( ) Não

10.1 - Caso tenha assinalado "Sim" no item acima, indique um exemplo. _____

_____

11-Você já ouviu falar em Criptografia? ( ) Sim ( ) Não

11.1 - Caso tenha assinalado "Sim" no item acima, indique onde ela está presente ou comente sobre o assunto.

_____

_____

_____

12- Você acredita que exista alguma relação entre a Criptografia e a Matemática?
( ) Sim ( ) Não

Comente.

_____

_____

_____

APÊNDICE B: Atividade de Sondagem – Teste Exploratório

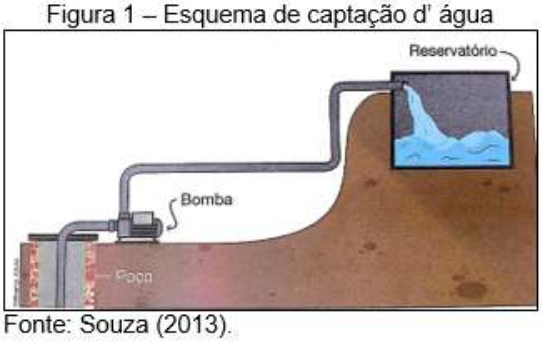
ATIVIDADE DE SONDAGEM – TESTE EXPLORATÓRIO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

Nome do aluno(a): _____ Data: __/__/____

1) (Souza, 2013, p.83 – Adaptada)[1] A água potável utilizada em propriedades rurais, de modo geral, é retirada de poços com auxílio de uma bomba-d'água elétrica. Em certo sítio, para abastecer o reservatório de água, é utilizada uma bomba-d'água com capacidade para bombear 10 litros por minuto. Essa bomba é ligada automaticamente quando o reservatório está com 175 litros de água e desligada ao enchê-lo (Figura 1).

Figura 1 – Esquema de captação d' água



Fonte: Souza (2013).

Com essas informações, podemos escrever uma fórmula que permite calcular a quantidade de água, em litros (ℓ), contida no reservatório em função do tempo (t) em que a bomba permanece ligada, considerando que não haja consumo de água durante esse período.

$$\ell = 10.t + 175$$

Utilizando essa fórmula, calcule a quantidade de água em:

a) 5 min

b) 13 min

[1] SOUZA, Joamir Roberto de. **Novo Olhar**: Matemática. 2. ed. São Paulo: FTD, 2013.

2) Dada a função f, com $f(x) = 5x + 2$, determine:

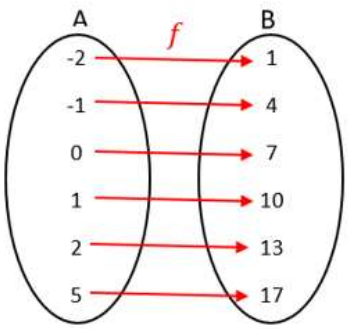
a) $f(-1)$

b) $f(0) + f(3)$

c) $f(9) - f(8)$

3) O salário de um vendedor de tênis é composto por uma parte fixa de R$ 1000,00, mais uma parte variável de R$ 3,00 por unidade vendida. Considerando que o salário do mês de dezembro foi de R$ 1438,00, quantos tênis foram vendidos nesse mês?

4) Seja f uma função afim definida por $f: A \to B$, com A={-2,-1,0,1,2,5} e B={1,4,7,10,13,17}. A partir do diagrama representado a seguir, determine:



a) $f^{-1}(4) =$

b) $f^{-1}(13) =$

5) Determine a inversa de cada função a seguir:

a) $f(x) = 6x - 1$

b) $f(x) = 7x + \frac{2}{3}$

APÊNDICE C: *Slides* (Apresentação da Criptografia e sua Evolução Histórica) – Teste Exploratório

Teste Exploratório
Trabalho de Conclusão de Curso

Karina França Bragança
Ramon Chagas Santos
Silvana Leal da Silva

Orientadora: Profª Me. Lívia Azelman de Faria Abreu
Coorientador: Profº Me. Alex Cabral Barbosa

Abril - 2017

CRIPTOGRAFIA

ESTEGANOGRAFIA

Do grego *steganos,* "coberto" e *graphein,* "escrita"

CITALE ESPARTANO

Figura 1 – Exemplo de Citale Espartano.

Fonte: Singh (2001, p. 24).

CÓDIGO

Substituição de palavras

Assassinato = D
Rei = Ω
Esta noite = 28

Assassinem o rei esta noite = D - Ω - 28

CIFRA

Substituição de letras

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

A M A N H E C E R
Z N Z M S V X V I

CIFRA DE CÉSAR

Mensagem original

MATEMATICA

Cifrando

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
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

Mensagem cifrada

P D W H P D W L F D

CIFRA DE CÉSAR

Mensagem cifrada

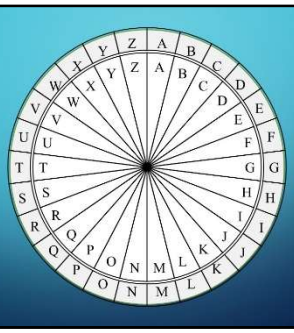
PDWHPDWLFD

Decifrando

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
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

Mensagem original

MA TEMA TICA



ATIVIDADE 1

Cifre a frase:

"O MAIOR SEGREDO É NÃO HAVER MISTÉRIO ALGUM."

utilizando a chave *deslocar 3 casas a frente.*

02:00

ATIVIDADE 1
RESPOSTA

Chave "deslocar 3 casas"

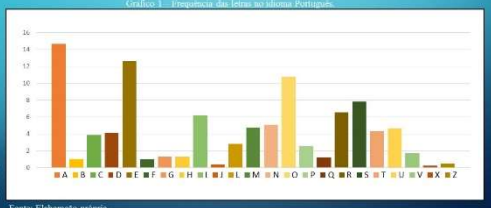
O	M	A	I	O	R		S	E	G	R	E	D	O		E		N	A	O
R	P	D	L	R	U		V	H	J	U	H	G	R		H		Q	D	R

H	A	V	E	R		M	I	S	T	E	R	I	O		A	L	G	U	M
K	D	Y	H	U		P	L	V	W	H	U	L	R		D	O	J	X	P

- CIFRA DE TRANSPOSIÇÃO
- CIFRA DE SUBSTITUIÇÃO

ANÁLISE DE FREQUÊNCIA

Gráfico 1 – Frequência das letras no idioma Português.



Fonte: Elaboração própria.

ATIVIDADE 2

Utilize a análise de frequência para descobrir o conteúdo da mensagem, sabendo que as letras que mais se repetem são F, P e B, não necessariamente nesta ordem.

"FTTB UFDOJDB QFSNJUF SFWFMBS B NFOTBHFN DSJQUPHSBGBEB, BOBMJTBOEP-TF B GSFRVFODJB EF DBSBDUFSFT OP UFYUP DJGSBEP EF BDPSEP DPN P JEJPNB VUJMJABEP."

05:00

ATIVIDADE 2
RESPOSTA

- Quantidade de letras:

F = 16 P = 11 B = 19

- Letras correspondentes:

F → E P → O B → A

ATIVIDADE 2
RESPOSTA

F	T	T	B		U	F	D	O	J	D	B		Q	F	S	N	J	U	F		S	F	W	F	M	B	S
E	S	S	A		T	E	C	N	I	C	A		P	E	R	M	I	T	E		R	E	V	E	L	A	R

B	N	F	O	T	B	H	F	N		D	S	J	Q	U	P	H	S	B	G	B	E	B
A	M	E	N	S	A	G	E	M		C	R	I	P	T	O	G	R	A	F	A	D	A

B	O	B	M	J	T	B	O	E	P		T	F		B		G	S	F	R	V	F	O	D	J	B		E	F
A	N	A	L	I	S	A	N	D	O		S	E		A		F	R	E	Q	U	E	N	C	I	A		D	E

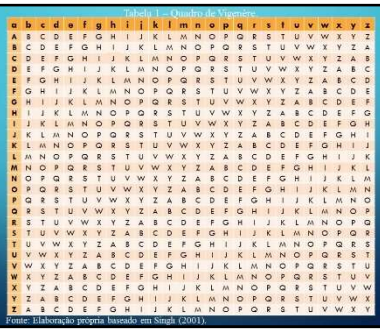
D	B	S	B	D	U	F	S	F	T		O	P		U	F	Y	U	P		D	J	G	S	B	E	P		E	F
C	A	R	A	C	T	E	R	E	S		N	O		T	E	X	T	O		C	I	F	R	A	D	O		D	E

B	D	P	S	E	P		D	P	N		P		J	E	J	P	N	B		V	U	J	M	J	A	B	E	P
A	C	O	R	D	O		C	O	M		O		I	D	I	O	M	A		U	T	I	L	I	Z	A	D	O

CRIPTOANALISTAS X CRIPTÓGRAFOS

CIFRA DE VIGENÈRE

Tabela 1 – Quadro de Vigenère



Fonte: Elaboração própria baseado em Singh (2001).

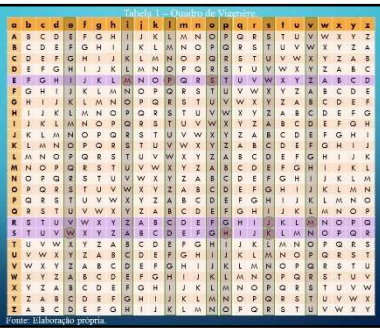
EXEMPLO

Cifrar a palavra POSSIVEL

Chave SER

P	O	S	S	I	V	E	L
S	E	R	S	E	R	S	E

Tabela 1 – Quadro de Vigenère



Fonte: Elaboração própria.

EXEMPLO

Cifrar a palavra POSSIVEL

Chave SER

P	O	S	S	I	V	E	L
S	E	R	S	E	R	S	E
H	S	J	K	M	M	W	P

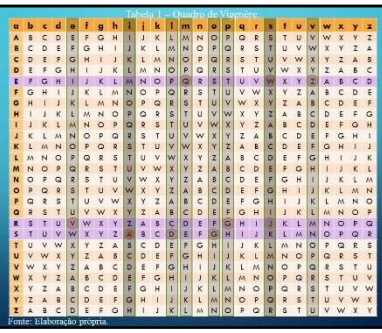
EXEMPLO

Decifrar a palavra AQGGWJAZVD

Chave SER

A	Q	G	G	W	J	A	Z	V	D
S	E	R	S	E	R	S	E	R	S

Tabela 1 – Quadro de Vigenère



Fonte: Elaboração própria.

EXEMPLO

Decifrar a palavra AQGGWJAZVD

Chave SER

A	Q	G	G	W	J	A	Z	V	D
S	E	R	S	E	R	S	E	R	S
I	M	P	O	S	S	I	V	E	L

ATIVIDADE 3

Decifre a mensagem:

"KYLF I XFWAZZMC. S QDTWJWQMIT RTMEEA UIUFVI DEQJ."

que utiliza a cifra de Vigenére e a chave REI.

ATIVIDADE 3
RESPOSTA

Chave "REI"

K	Y	L	F	I	X	F	W	A	Z	Z	M	C	S	Q	D	T	W	J	W	Q	M	I	T
R	E	I	R	E	I	R	E	I	R	E	I	R	E	I	R	E	I	R	E	I	R	E	I

R	T	M	E	E	A
R	E	I	R	E	I

U	I	U	F	V	I
R	E	I	R	E	I

D	E	Q	J
R	E	I	R

Tabela 1 – Quadro de Vigenère

	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: Elaboração própria.

ATIVIDADE 3
RESPOSTA

Chave "REI"

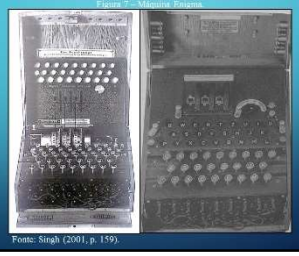
K	Y	L	F	I	X	F	W	A	Z	Z	M	C	S	Q	D	T	W	J	W	Q	M	I	T
R	E	I	R	E	I	R	E	I	R	E	I	R	E	I	R	E	I	R	E	I	R	E	I
T	U	D	O	E	P	O	S	S	I	V	E	L	O	I	M	P	O	S	S	I	V	E	L

R	T	M	E	E	A
R	E	I	R	E	I
A	P	E	N	A	S

U	I	U	F	V	I
R	E	I	R	E	I
D	E	M	O	R	A

D	E	Q	J
R	E	I	R
M	A	I	S

MÁQUINA ENIGMA



Fonte: Singh (2001, p. 159).

BOMBAS DE TURING

- POPULARIZAÇÃO DOS COMPUTADORES
- PROBLEMA DA DISTRIBUIÇÃO DE CHAVES
- DIFFIE-HELLMAN-MERKLE

Karina

Silvana

Ramon

CHAVE SIMÉTRICA

Cifrar

Decifrar

CHAVE ASSIMÉTRICA

Chave Pública

Cifrar

Chave Privada

Decifrar

CRIPTOGRAFIA RSA

Ron Rivest, Adi Shamir e Leonard Adleman

ARITMÉTICA MODULAR

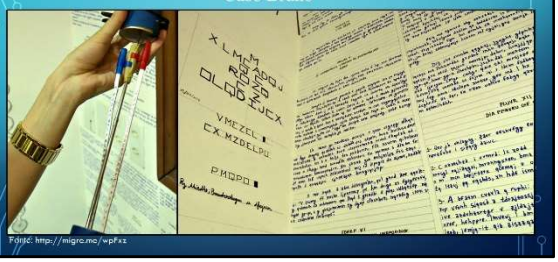
$4 = 25 \pmod 7$

$4 = 32 \pmod 7$

CRIPTOGRAFIA NA ATUALIDADE

CRIPTOGRAFIA NA ATUALIDADE

Caso Bruno



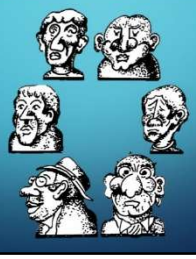
Fonte: http://migre.me/wpFxz

GINCANA

TAREFA 1

Esteganografia

Indique a sequência dos rostos.



03:00

Indique a sequência dos rostos.
RESPOSTA

TAREFA 2

Citale Espartano

Descubra a mensagem escondida.

03:00

Descubra a mensagem escondida.
RESPOSTA

Frase 1: A CRIPTOGRAFIA UTILIZA MÉTODOS

Frase 2: PARA TRANSFORMAR UMA

Frase 3: MENSAGEM EM UM CÓDIGO.

TAREFA 3

Diffie – Hellman - Merkle

Encontre a sequência correta da mensagem.

Encontre a sequência correta da mensagem.
RESPOSTA

15 7 55

TAREFA 4

Teste de Força Bruta

Fonte: http://migre.me/wpEzb

APÊNDICE D: Atividade de Investigação – Teste Exploratório

ATIVIDADES – TESTE EXPLORATÓRIO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

Nome do aluno(a): _____ Data: __/__/____

1) Cifre numericamente o nome da escola.

I	N	S	T	I	T	U	T	O

F	E	D	E	R	A	L

F	L	U	M	I	N	E	N	S	E

2) (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?

3) Utilizando a palavra CODIGO:

   a) Indique a sequência numérica associada;

   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?

4) Cifre a palavra CRIPTOGRAFIA, utilizando a função cifradora $f(x) = 3x + 1$.

5) A mensagem TMAC AMLQCESGS foi cifrada a partir da função cifradora $f(x) = x - 2$. Você seria capaz de descobrir a mensagem original?

6) A palavra VESTIBULAR foi cifrada utilizando uma função cuja inversa é $f^{-1}(x) = \frac{x-4}{2}$. Qual a função cifradora utilizada, e qual a mensagem?

APÊNDICE E: *Slides* (Atividade de Investigação) – Teste Exploratório

Teste Exploratório
Trabalho de Conclusão de Curso

Karina França Bragança
Ramon Chagas Santos
Silvana Leal da Silva

Orientadora: Profª Me. Lívia Azelman de Faria Abreu
Coorientador: Profº Me. Alex Cabral Barbosa

Abril - 2017

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	26

Cifre: INSTITUTO FEDERAL FLUMINENSE

I	N	S	T	I	T	U	T	O
9	14	19	20	9	20	21	20	15

F	E	D	E	R	A	L
6	5	4	5	18	1	12

F	L	U	M	I	N	E	N	S	E
6	12	21	13	9	14	5	14	19	5

Exemplo (OBMEP, 2007 – adaptada): Utilizando a chave 5, a palavra PAI é cifrada como 20 – 5 – 13.

1. Cifre OBMEP usando a chave 20.

Resposta: 8 – 21 – 6 – 24 – 9

2. Usando a chave 7, descubra qual palavra foi cifrada como

14 – 12 – 22 – 20 – 12 – 27 – 25 – 16 – 8.

Resposta: GEOMETRIA

3. Bernardo codificou uma palavra de 4 letras com a chave 20, 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 codificou.

4. Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?

RESPOSTAS

3. Bernardo codificou uma palavra de 4 letras com a chave 20, 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 codificou.

26 – 20 – 13 – 8 GATO

4. Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?

Chave "avance 24 casas"

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	26

CODIGO

C	O	D	I	G	O
3	15	4	9	7	15

Chave "avance 4 casas"

C	O	D	I	G	O
7	19	8	13	11	19

Mensagem Cifrada

7	19	8	13	11	19
G	S	H	M	K	S

Expressão Matemática: $f(x) = x + 4$

E quando ultrapassa de 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
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	26

Ā	B̄	C̄	D̄	Ē	F̄	Ḡ	H̄	Ī	J̄	K̄	L̄	M̄	N̄	Ō	P̄	Q̄	R̄	S̄	T̄	Ū	V̄	W̄	X̄	Ȳ	Z̄
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52

Ā	B̄	C̄	D̄	Ē	F̄	Ḡ	H̄	Ī	J̄	K̄	L̄	M̄	N̄	Ō	P̄	Q̄	R̄	S̄	T̄	Ū	V̄	W̄	X̄	Ȳ	Z̄
53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	...

CRIPTOGRAFIA

C	R	I	P	T	O	G	R	A	F	I	A
3	18	9	16	20	15	7	18	1	6	9	1

Chave $f(x) = 3x + 1$

C	R	I	P	T	O	G	R	A	F	I	A
10	55	28	49	61	46	22	55	4	19	28	4

Mensagem Cifrada

10	55	28	49	61	46	22	55	4	19	28	4
J	C̄	B̄	W̄	Ī	T̄	V	C̄	D	S	B̄	D

TMAC AMLQCESGS

T	M	A	C
20	13	1	3

A	M	L	Q	C	E	S	G	S
1	13	12	17	3	5	19	7	19

Chave $f(x) = x - 2$

Para decifrar utiliza-se $f^{-1}(x) = x + 2$

T	M	A	C
22	15	3	5

A	M	L	Q	C	E	S	G	S
3	15	14	19	5	7	21	9	21

Mensagem Original

22	15	3	5
V	O	C	E

3	15	14	19	5	7	21	9	21
C	O	N	S	E	G	U	I	U

VESTIBULAR

V	E	S	T	I	B	U	L	A	R
22	5	19	20	9	2	21	12	1	18

$f^{-1}(x) = \dfrac{x-4}{2}$ Chave para cifrar: $f(x) = 2x + 4$

V	E	S	T	I	B	U	L	A	R
48	14	42	44	22	8	46	28	6	40

Mensagem Cifrada

48	14	42	44	22	8	46	28	6	40
V̄	N	P̄	R̄	V	H	T̄	B	F	N̄

APÊNDICE F: Atividade de Verificação – Teste Exploratório

ATIVIDADES – TESTE EXPLORATÓRIO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

Nome do aluno(a): _____ Data: __/__/____

1) Questão (Fatec – 2017): Maria, aluna da Fatec Mococa, para garantir a segurança das mensagens que pretende transmitir, criou um sistema de criptografia da seguinte forma:

- montou uma tabela de 2 linhas e 13 colunas para colocar as 26 letras do alfabeto, sem repetição de letra;
- nas cinco células iniciais da 1ª linha, da esquerda para a direita, escreveu, uma a uma, as letras F, A, T, E, C nessa ordem;
- ainda na 1ª linha, na 6ª célula, da esquerda para a direita, obedecendo a ordem alfabética (de A a Z) colocou a primeira letra ainda não utilizada nas células anteriores;
- da 7ª célula a 13ª célula da 1ª linha, inseriu sete letras, da esquerda para a direita, sem repetir letra, seguindo a ordem alfabética, começando pela primeira letra ainda não utilizada nas células anteriores;
- preencheu a 2ª linha, da esquerda para a direita, com as letras restantes do alfabeto, também em ordem alfabética e sem repetição de qualquer letra já utilizada anteriormente.

A tabela mostra o início do processo, com as seis primeiras letras.

F	A	T	E	C	B							

Tendo construído a tabela conforme o descrito, para criptografar uma mensagem, Maria substitui cada letra da 1ª linha pela que está na 2ª linha, na mesma coluna, e vice-versa. A acentuação, a pontuação e o espaço entre as palavras são desconsiderados.

Assim, para desejar BOA PROVA para uma colega, que sabia fazer a decodificação, escreveu RTNEBTHN.

Para João, que também sabia decodificar a mensagem, Maria escreveu:

AGAQNENBPSPNEBPASPB

A partir da decodificação, João entendeu que a mensagem de Maria foi:

a) Nunca pare de aprender
b) Nunca deixe de estudar
c) Nunca faça isso de novo
d) Sempre tire boas notas
e) Sempre faça boas ações

2) Cifre a frase O SEGREDO NAO SERA REVELADO, utilizando a chave "avance 5 casas", e indique como a chave cifradora poderia ser escrita em linguagem matemática.

3) A palavra MATEMATICA foi cifrada por João utilizando uma chave cuja função decifradora é $f^{-1}(x) = x - 7$. Qual a função cifradora utilizada, e como ficou a mensagem?

4) Henrique recebeu uma carta misteriosa contendo a seguinte mensagem:

TUGFY GEHJHUGY YMYLRY Y LKQFU.

E junto a mensagem havia três funções, das quais uma delas foi utilizada para cifrar a mensagem.

$$f(x) = x + 5$$

$$f(x) = -x + 26$$

$$f(x) = x - 4$$

Qual a mensagem original da carta?

APÊNDICE G: Questionário Final – Teste Exploratório

QUESTIONÁRIO II – TESTE EXPLORATÓRIO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

1- Nome do aluno(a): _____

2- Com base na escala abaixo:

D	Discordo
DP	Discordo parcialmente
NC ND	Não Concordo nem discordo
CP	Concordo parcialmente
C	Concordo

Em sua opinião, o estudo acerca do Tema Criptografia:

	D	DP	NC ND	CP	C
Foi interessante.					
Agregou novo conhecimento.					
Apresentou relação com conteúdos Matemáticos.					
Apresentou linguagem clara.					
Foi apresentado de maneira atraente.					
Foi um estudo diferenciado.					
Possibilitou a percepção deste tema no cotidiano.					
Contribuiu no estudo de função afim.					

Contribuiu no estudo de função inversa da função afim.					
Tornou o estudo de função inversa mais significativo.					
Permitiu estabelecer relação do tema com a função afim e sua inversa.					
Seria interessante abordar esse tema em sala de aula.					

O espaço a seguir é para comentários relacionados a qualquer afirmativa acima. Caso tenha assinalado a coluna D, DP ou NC ND para alguma(s) afirmativa(s), por favor, mencione o(s) motivo(s) que levaram a essa opção.

3- Acerca desse estudo, comente pontos positivos e negativos.

APÊNDICE H: Ficha 1 (Atividade da Cifra de César) – Teste Exploratório

Nome: _____

ATIVIDADE 1 - TESTE EXPLORATÓRIO

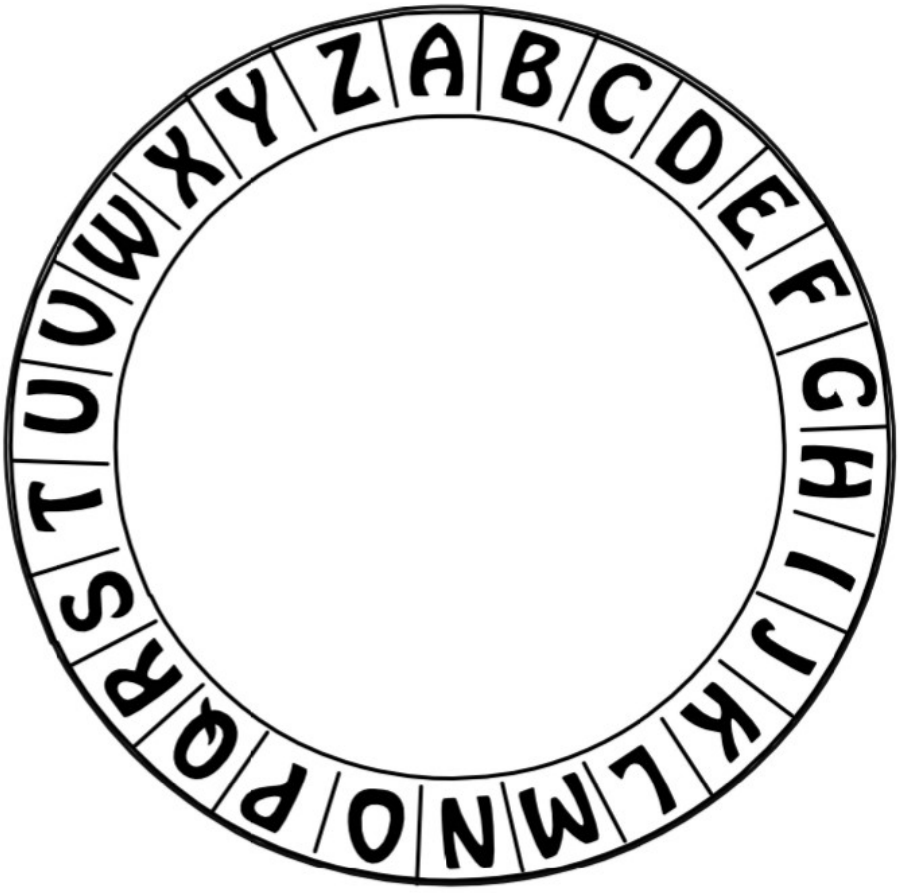
Cifre a frase “O maior segredo é não haver mistério algum.” utilizando a chave *deslocar 3 casas a frente.*

O		M	A	I	O	R		S	E	G	R	E	D	O		E		N	A	O

H	A	V	E	R		M	I	S	T	E	R	I	O		A	L	G	U	M

APÊNDICE I: Disco (Letra com Letra)


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 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

APÊNDICE J: Ficha 2 (Atividade de Análise de Frequência) – Teste Exploratório

Nome: ____

ATIVIDADE 2 - TESTE EXPLORATÓRIO

Utilize a análise de frequência para descobrir o conteúdo da mensagem, sabendo que as letras que mais se repetem são F, P e B, não necessariamente nesta ordem.

F T T B   U F D O J D B   Q F S N J U F

S F W F M B S   B   N F O T B H F N

D S J Q U P H S B G B E B   B O B M J T B O E P

T F   B   G S F R V F O D J B   E F

D B S B D U F S F T   O P   U F Y U P

D J G S B E P   E F   B D P S E P   D P N

P   J E J P N B   V U J M J A B E P

APÊNDICE K: Ficha 3 (Atividade da Cifra de Vigenère) – Teste Exploratório

Nome: _____

ATIVIDADE 3 - TESTE EXPLORATÓRIO

Decifre a mensagem "KYLF I XFWAZZMC. S QDTWJWQMIT RTMEEA UIUFVI DEQJ." que foi cifrada utilizando a cifra de Vigenère e a chave REI.

K	Y	L	F

I

X	F	W	A	Z	Z	M	C

S

Q	D	T	W	J	W	Q	M	I	T

R	T	M	E	E	A

U	I	U	F	V	I

D	E	Q	J

APÊNDICE L: Quadrado de Vigenère

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA Fluminense — MINISTÉRIO DA EDUCAÇÃO — BRASIL — DIRLIC — matemática LICENCIATURA

CIFRA DE VIGENÈRE

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

APÊNDICE M: Sequência das Faces e Ficha 4 (Atividade de Esteganografia) – Teste Exploratório






INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA Fluminense — MINISTÉRIO DA EDUCAÇÃO — BRASIL GOVERNO FEDERAL — DIRLIC — matemática LICENCIATURA

GINCANA – TESTE EXPLORATÓRIO

Estas cabeças formam uma série, podendo ordenar-se da primeira à sexta segundo uma regra lógica. Qual é essa regra? Cole as imagens na sequência correta.

APÊNDICE N: Ficha de Resposta em Formato de Cadeado


TCC
RSK

APÊNDICE O: Fichas em Formato Chaves (Atividade de Diffie-Hellman-Merkle)


15743

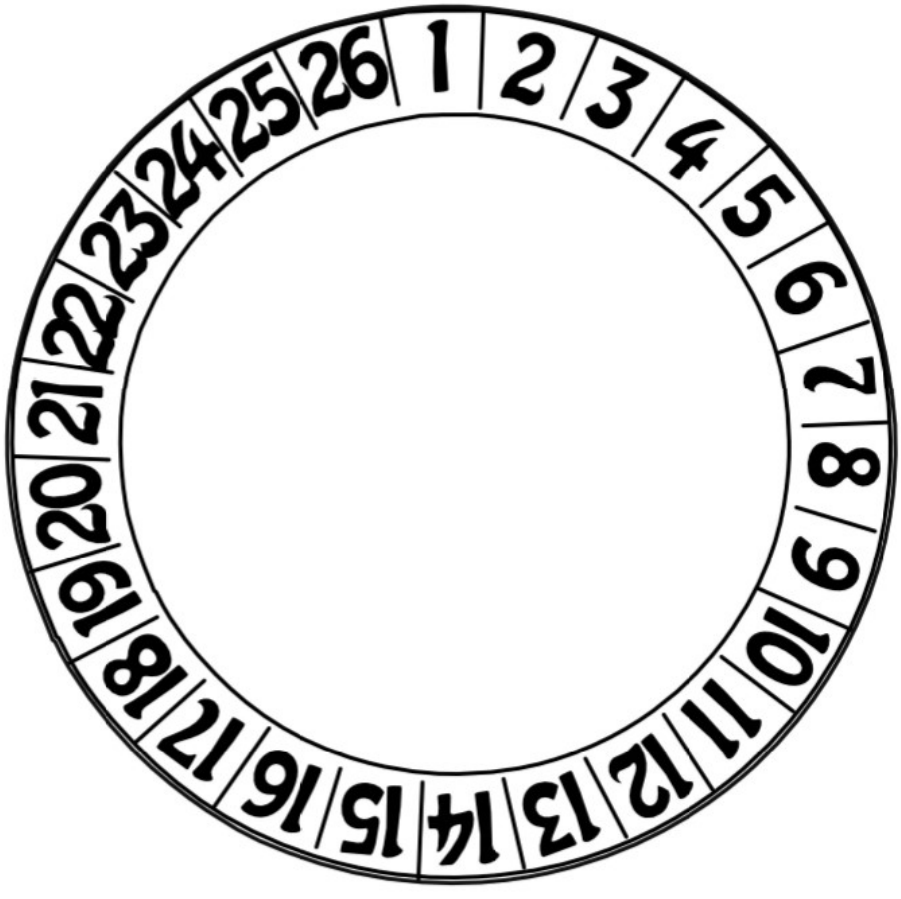

15752


15755


15757

APÊNDICE P: Disco (Letra com Número)


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 26

APÊNDICE Q: Questionário Inicial – Experimentação

QUESTIONÁRIO I – EXPERIMENTAÇÃO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

1- Nome do aluno(a): _____

2- Sexo: ( ) Masculino ( ) Feminino

3- Idade: _____

4- Cursou o 9º ano do ensino fundamental em: ( ) escola particular ( ) escola pública

5- Você se interessa por Matemática? ( ) Sim ( ) Não
Comente.
_____
_____
_____

6- Você considera a Matemática uma disciplina importante? ( ) Sim ( ) Não
Comente.
_____
_____
_____

7- Você consegue perceber a utilização da Matemática em seu cotidiano? ( ) Sim ( ) Não

7.1 - Caso tenha assinalado "Sim" no item acima, indique um exemplo. _____

_____

8- Você já estudou função afim? ( ) Sim ( ) Não

9- Você já estudou função inversa? ( ) Sim ( ) Não

Caso tenha assinalado "Sim" no item 9, responda o item abaixo.

10- Ao estudar a função inversa, foi apresentada alguma aplicação sobre esse tema?
( ) Sim ( ) Não

10.1 - Caso tenha assinalado "Sim" no item acima, indique um exemplo. _____

_____

11-Você já ouviu falar em Criptografia? ( ) Sim ( ) Não

11.1 - Caso tenha assinalado "Sim" no item acima, indique onde ela está presente ou comente sobre o assunto.

_____

_____

_____

12- Você considera que exista alguma relação entre a Criptografia e a Matemática?
( ) Sim ( ) Não

Comente.

_____

_____

_____

APÊNDICE R: Atividade de Sondagem – Experimentação

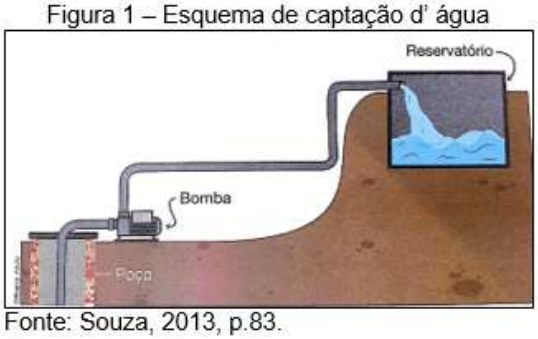
ATIVIDADE DE SONDAGEM – EXPERIMENTAÇÃO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

Nome do aluno(a): _____ Data: __/__/____

1) (SOUZA, 2013, p.83 – Adaptada)[1] A água potável utilizada em propriedades rurais, de modo geral, é retirada de poços com auxílio de uma bomba-d'água elétrica. Em certo sítio, para abastecer o reservatório de água, é utilizada uma bomba-d'água com capacidade para bombear 10 litros por minuto. Essa bomba é ligada automaticamente quando o reservatório está com 175 litros de água e desligada ao enchê-lo (Figura 1).

Figura 1 – Esquema de captação d' água



Fonte: Souza, 2013, p.83.

Com essas informações, podemos escrever uma fórmula que permite calcular a quantidade (q) de água, em litros, contida no reservatório em função do tempo (t), em minutos, em que a bomba permanece ligada, considerando que não haja consumo de água durante esse período.

$$q = 10\,t + 17$$

Utilizando essa fórmula, calcule a quantidade de água em:

a) 5 min

b) 13 min

[1] SOUZA, Joamir Roberto de. **Novo Olhar**: Matemática. 2. ed. São Paulo: FTD, 2013.

2) Dada a função f, com $f(x) = 5x + 2$, determine:

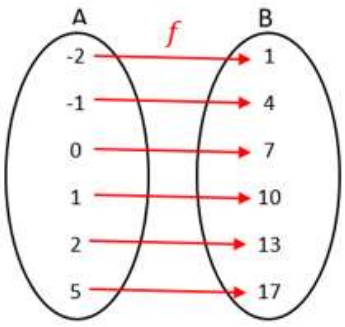
a) $f(-1)$

b) $f(0) + f(3)$

c) $f(9) - f(8)$

3) O salário de um vendedor de tênis é composto por uma parte fixa de R$ 1000,00, mais uma parte variável de R$ 3,00 por unidade vendida. Considerando que o salário do mês de dezembro foi de R$ 1438,00, quantos tênis foram vendidos nesse mês?

4) Seja f uma função afim definida por $f: A \to B$, com A={-2,-1,0,1,2,5} e B={1,4,7,10,13,17}. A partir do diagrama representado a seguir, determine:



a) $f^{-1}(4) =$

b) $f^{-1}(13) =$

5) Considerando as funções $f: \mathbb{R} \to \mathbb{R}$ e $g: \mathbb{R} \to \mathbb{R}$, determine a inversa de cada função a seguir.

a) $f(x) = 6x - 1$

b) $g(x) = 7x + \frac{2}{3}$

APÊNDICE S: *Slides* (Apresentação da Criptografia e sua Evolução Histórica) – Experimentação

Experimentação
Trabalho de Conclusão de Curso

Karina França Bragança
Ramon Chagas Santos
Silvana Leal da Silva

Orientadora: Profª Me. Lívia Azelman de Faria Abreu
Coorientador: Profº Me. Alex Cabral Barbosa

Abril - 2017

CRIPTOGRAFIA

ESTEGANOGRAFIA

Do grego *steganos,* "coberto" e *graphein,* "escrita"

CITALE ESPARTANO

Figura 1 – Exemplo de Citale Espartano.

Fonte: Singh (2001, p. 24).

CÓDIGO

Substituição de palavras

Assassinato = D
Rei = Ω
Esta noite = 28

Assassinem o rei esta noite = D - Ω - 28

CIFRA

Substituição de letras

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

A M A N H E C E R
Z N Z M S V X V I

CIFRA DE CÉSAR

Mensagem original

MATEMATICA

Cifrando

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
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

Mensagem cifrada

P D W H P D W L F D

CIFRA DE CÉSAR

Mensagem cifrada

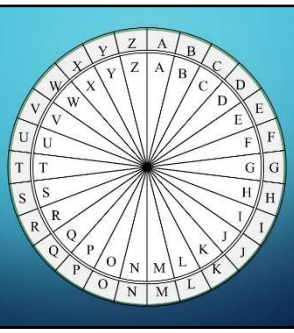
PDWHPDWLFD

Decifrando

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
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

Mensagem original

MA TEMA TICA



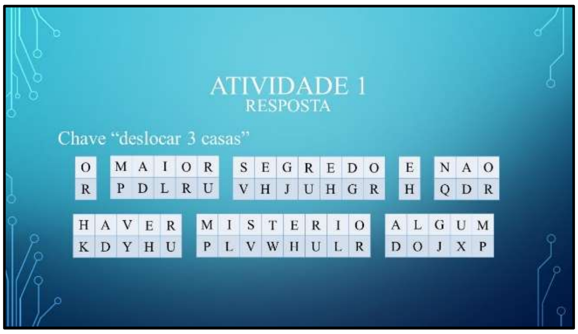
ATIVIDADE 1

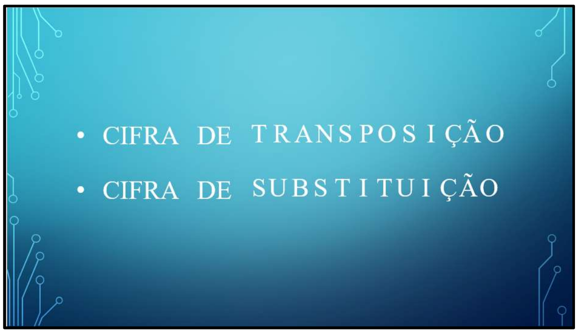
Cifre a frase:

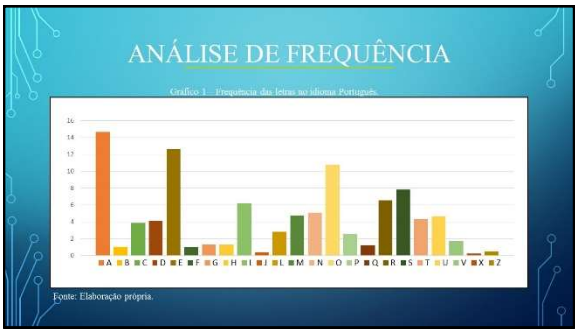
"O MAIOR SEGREDO É NÃO HAVER MISTÉRIO ALGUM."

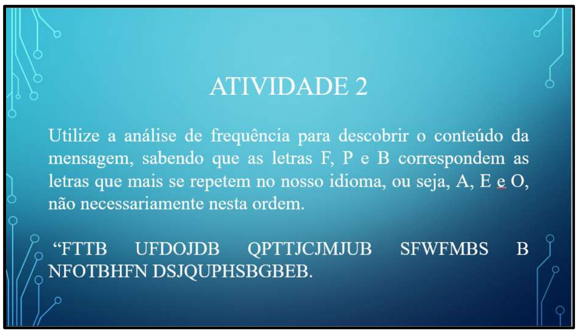
utilizando a chave *deslocar 3 casas a frente.*


05:00

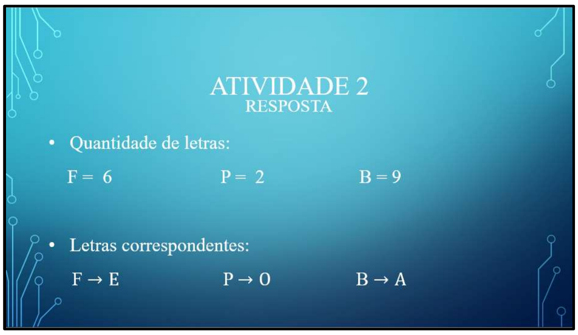

ATIVIDADE 1
RESPOSTA
Chave "deslocar 3 casas"
O MAIOR SEGREDO E NAO
R PDLRU VHJUHGR H QDR
HAVER MISTERIO ALGUM
KDYHU PLVWHULR DOJXP


CIFRA DE TRANSPOSIÇÃO
CIFRA DE SUBSTITUIÇÃO


ANÁLISE DE FREQUÊNCIA
Fonte: Elaboração própria.


ATIVIDADE 2
Utilize a análise de frequência para descobrir o conteúdo da mensagem, sabendo que as letras F, P e B correspondem as letras que mais se repetem no nosso idioma, ou seja, A, E e O, não necessariamente nesta ordem.
"FTTB UFDOJDB QPTTJCJMJUB SFWFMBS B NFOTBHFN DSJQUPHSBGBEB.


10:00


ATIVIDADE 2
RESPOSTA
Quantidade de letras:
F = 6
P = 2
B = 9
Letras correspondentes:
F → E
P → O
B → A


ATIVIDADE 2
RESPOSTA
FTTB UFDOJDB
ESSA TECNICA
QPTTJCJMJUB SFWFMBS
POSSIBILITA REVELAR
B NFOTBHFN DSJQUPHSBGBEB
A MENSAGEM CRIPTOGRAFADA


CRIPTOANALISTAS X CRIPTÓGRAFOS


CIFRA DE VIGENÈRE

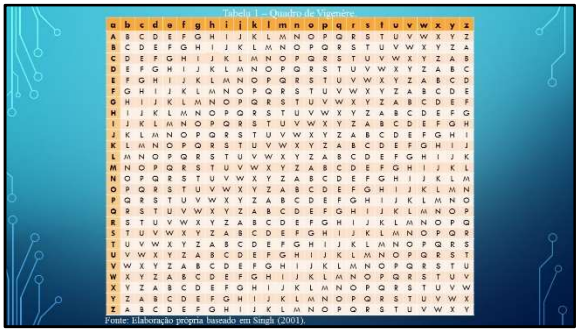
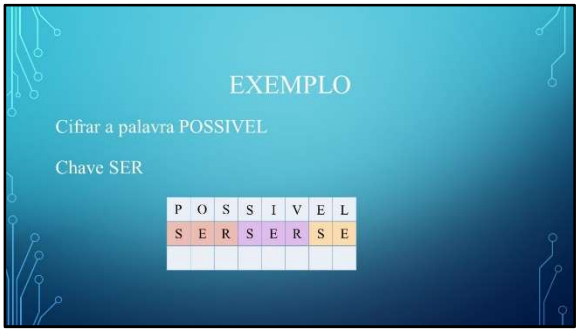


Tabela 1 – Quadro de Vigenère
Fonte: Elaboração própria baseado em Singh (2001).


EXEMPLO
Cifrar a palavra POSSIVEL
Chave SER
P O S S I V E L
S E R S E R S E

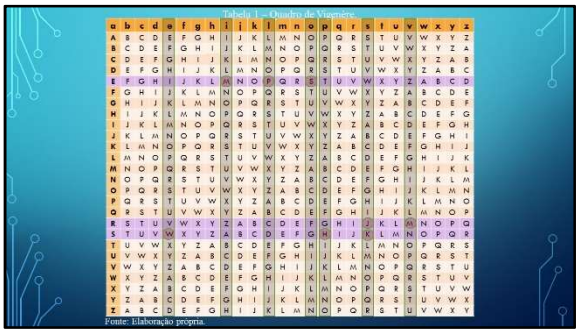
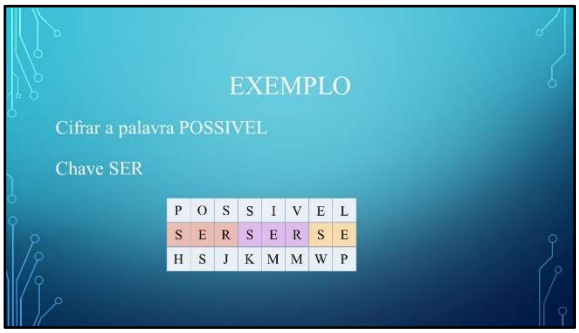


Tabela 1 – Quadro de Vigenère
Fonte: Elaboração própria.


EXEMPLO
Cifrar a palavra POSSIVEL
Chave SER
P O S S I V E L
S E R S E R S E
H S J K M M W P


EXEMPLO
Decifrar a palavra EIEKEXWQ
Chave SER
E I E K E X W Q
S E R S E R S E

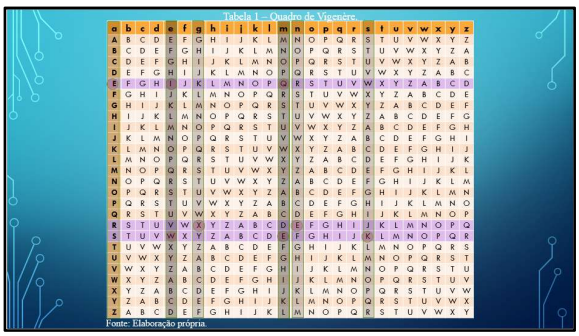
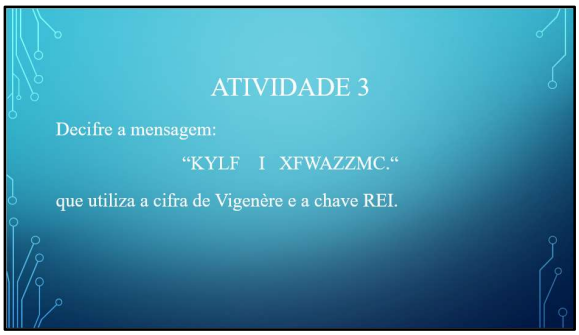


Tabela 1 – Quadro de Vigenère
Fonte: Elaboração própria.


EXEMPLO
Decifrar a palavra EIEKEXWQ
Chave SER
E I E K E X W Q
S E R S E R S E
M E N S A G E M


ATIVIDADE 3
Decifre a mensagem:
“KYLF I XFWAZZMC.“
que utiliza a cifra de Vigenère e a chave REI.


05:00


ATIVIDADE 3
RESPOSTA
Chave “REI”
K Y L F
R E I R
I
E
X F W A Z Z M C
I R E I R E I R

Tabela 1 – Quadro de Vigenère.

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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: Elaboração própria.

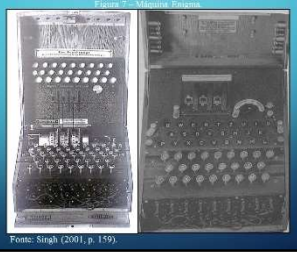
ATIVIDADE 3
RESPOSTA

Chave "REI"

K	Y	L	F		I		X	F	W	A	Z	Z	M	C
R	E	I	R		E		I	R	E	I	R	E	I	R
T	U	D	O		E		P	O	S	S	I	V	E	L

MÁQUINA ENIGMA

Figura 7 – Máquina Enigma



Fonte: Singh (2001, p. 159).

BOMBAS DE TURING

- POPULARIZAÇÃO DOS COMPUTADORES
- PROBLEMA DA DISTRIBUIÇÃO DE CHAVES
- DIFFIE-HELLMAN-MERKLE

CHAVE SIMÉTRICA

CHAVE ASSIMÉTRICA

CRIPTOGRAFIA RSA

Ron Rivest, Adi Shamir e Leonard Adleman

CRIPTOGRAFIA NA ATUALIDADE

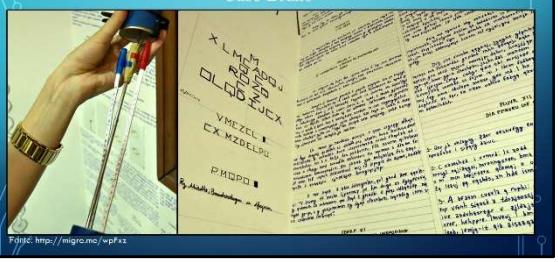
CRIPTOGRAFIA NA ATUALIDADE

Figura 3 – Exemplos de aplicações da Criptografia

Fonte: Elaboração própria.

CRIPTOGRAFIA NA ATUALIDADE

Caso Bruno

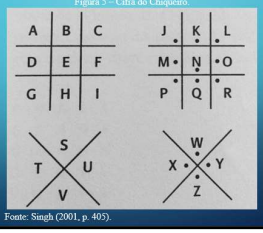


Fonte: http://migre.me/wpFxz

CRIPTOGRAFIA NA ATUALIDADE

Cifra do Chiqueiro

Figura 5 – Cifra do Chiqueiro.



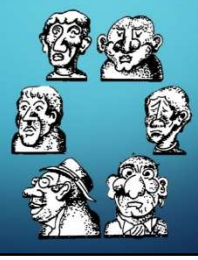
Fonte: Singh (2001, p. 405).

GINCANA

TAREFA 1

Esteganografia

Indique a sequência dos rostos.



03:00

Indique a sequência dos rostos.
RESPOSTA

TAREFA 2

Citale Espartano

Descubra a mensagem escondida.

03:00

Descubra a mensagem escondida.
RESPOSTA

Frase 1: A CRIPTOGRAFIA UTILIZA MÉTODOS

Frase 2: PARA TRANSFORMAR UMA

Frase 3: MENSAGEM EM UM CÓDIGO.

TAREFA 3

Teste de Força Bruta

Figura 6 – Chaves e Cadeado

Fonte: http://mgre.me/wpFzb

APÊNDICE T: Ficha 2 (Atividade de Análise de Frequência) – Experimentação

Nome: _____

ATIVIDADE 2 - EXPERIMENTAÇÃO

Utilize a análise de frequência para descobrir o conteúdo da mensagem, sabendo que as letras que mais se repetem são F, P e B, não necessariamente nesta ordem.

F	T	T	B

U	F	D	O	J	D	B

Q	P	T	T	J	C	J	M	J	U	B

S	F	W	F	M	B	S

B

N	F	O	T	B	H	F	N

D	S	J	Q	U	P	H	S	B	G	B	E	B

APÊNDICE U: Ficha 3 (Atividade da Cifra de Vigenère) – Experimentação

Nome: _____

ATIVIDADE 3 - EXPERIMENTAÇÃO

Decifre a mensagem "KYLF I XFWAZZMC. S QDTWJWQMIT RTMEEA UIUFVI DEQJ." que foi cifrada utilizando a cifra de Vigenère e a chave REI.

K	Y	L	F

I

X	F	W	A	Z	Z	M	C

APÊNDICE V: Ficha 1 (Atividade da Cifra de César) – Experimentação

Nome: _____

ATIVIDADE 1 - EXPERIMENTAÇÃO

Cifre a frase "O maior segredo é não haver mistério algum. " utilizando a chave *deslocar 3 casas a frente.*

O		M	A	I	O	R		S	E	G	R	E	D	O		E		N	A	O

H	A	V	E	R		M	I	S	T	E	R	I	O		A	L	G	U	M

APÊNDICE W: Ficha 4 (Atividade de Esteganografia) – Experimentação

GINCANA – EXPERIMENTAÇÃO

Estas cabeças formam uma série, podendo ordenar-se da primeira à sexta segundo uma regra lógica. Qual é essa regra? Cole as imagens na sequência correta.

APÊNDICE X: Atividade de Investigação – Experimentação

ATIVIDADE INVESTIGATIVA – EXPERIMENTAÇÃO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

Nome do aluno(a): _____ Data: __/__/____

1) Cifre numericamente o nome da escola.

D	O	M

O	T	A	V	I	A	N	O

2) 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?

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

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

5) A palavra V E S T I B U L A R foi cifrada utilizando uma função cifradora $f: \mathbb{Z} \to \mathbb{Z}$ cuja inversa é $f^{-1}(x) = \frac{x-4}{2}$. Qual a função cifradora utilizada, e qual a mensagem?

6) (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?

APÊNDICE Y : *Slides* (Atividade de Investigação) – Experimentação

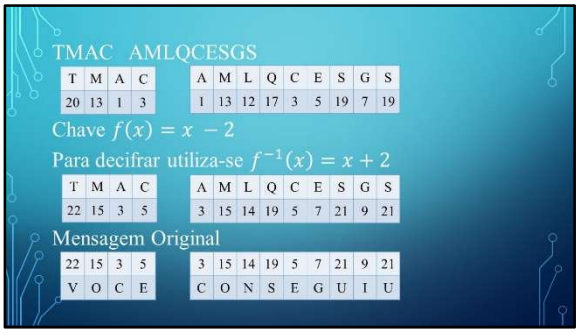

Experimentação
Trabalho de Conclusão de Curso
Karina França Bragança
Ramon Chagas Santos
Silvana Leal da Silva
Orientadora: Profª Me. Lívia Azelman de Faria Abreu
Coorientador: Profº Me. Alex Cabral Barbosa
Abril - 2017

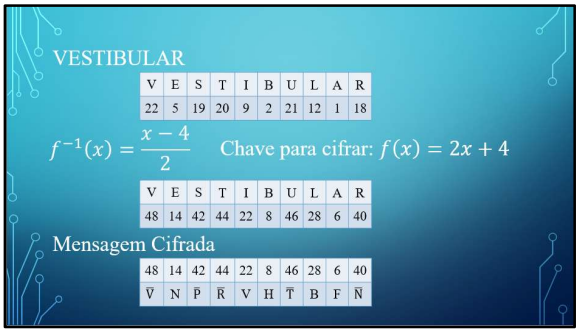

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Cifre: DOM OTAVIANO
D O M
4 15 13
O T A V I A N O
15 20 1 22 9 1 14 15

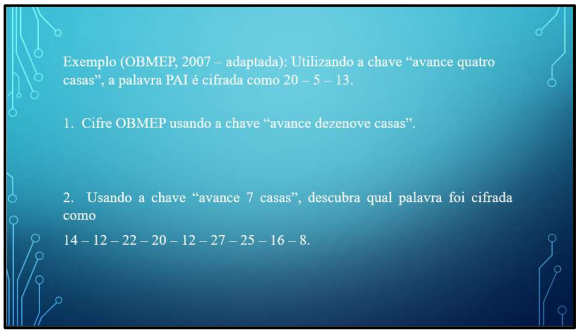

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
CODIGO
C O D I G O
3 15 4 9 7 15
Chave "avance 4 casas"
C O D I G O
7 19 8 13 11 19
Mensagem Cifrada
7 19 8 13 11 19
G S H M K S
Expressão Matemática: $f(x) = x + 4$

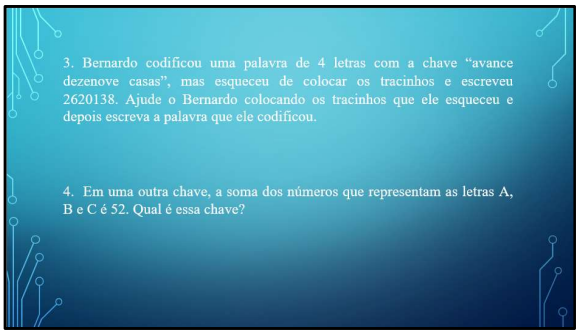

E quando ultrapassa de 26?
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Ā B̄ C̄ D̄ Ē F̄ Ḡ H̄ Ī J̄ K̄ L̄ M̄ N̄ Ō P̄ Q̄ R̄ S̄ T̄ Ū V̄ W̄ X̄ Ȳ Z̄
27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Ā B̄ C̄ D̄ Ē F̄ Ḡ H̄ Ī J̄ K̄ L̄ M̄ N̄ Ō P̄ Q̄ R̄ S̄ T̄ Ū V̄ W̄ X̄ Ȳ Z̄
53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 ...

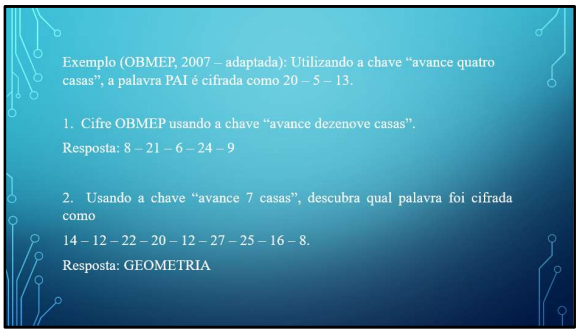

CRIPTOGRAFIA
C R I P T O G R A F I A
3 18 9 16 20 15 7 18 1 6 9 1
Chave $f(x) = 3x + 1$
C R I P T O G R A F I A
10 55 28 49 61 46 22 55 4 19 28 4
Mensagem Cifrada
10 55 28 49 61 46 22 55 4 19 28 4
J C̄ B̄ W̄ Ī T̄ V C̄ D S B̄ D

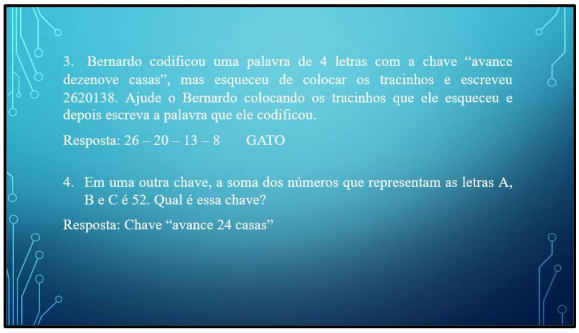

TMAC AMLQCESGS
T M A C
20 13 1 3
A M L Q C E S G S
1 13 12 17 3 5 19 7 19
Chave $f(x) = x - 2$
Para decifrar utiliza-se $f^{-1}(x) = x + 2$
T M A C
22 15 3 5
A M L Q C E S G S
3 15 14 19 5 7 21 9 21
Mensagem Original
22 15 3 5
V O C E
3 15 14 19 5 7 21 9 21
C O N S E G U I U


VESTIBULAR
V E S T I B U L A R
22 5 19 20 9 2 21 12 1 18
$f^{-1}(x) = \frac{x-4}{2}$ Chave para cifrar: $f(x) = 2x + 4$
V E S T I B U L A R
48 14 42 44 22 8 46 28 6 40
Mensagem Cifrada
48 14 42 44 22 8 46 28 6 40
V̄ N P̄ R̄ V H T̄ B F N̄


Exemplo (OBMEP, 2007 – adaptada): Utilizando a chave "avance quatro casas", a palavra PAI é cifrada como 20 – 5 – 13.
1. Cifre OBMEP usando a chave "avance dezenove casas".
2. Usando a chave "avance 7 casas", descubra qual palavra foi cifrada como
14 – 12 – 22 – 20 – 12 – 27 – 25 – 16 – 8.


3. Bernardo codificou 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 codificou.
4. Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?


Exemplo (OBMEP, 2007 – adaptada): Utilizando a chave "avance quatro casas", a palavra PAI é cifrada como 20 – 5 – 13.
1. Cifre OBMEP usando a chave "avance dezenove casas".
Resposta: 8 – 21 – 6 – 24 – 9
2. Usando a chave "avance 7 casas", descubra qual palavra foi cifrada como
14 – 12 – 22 – 20 – 12 – 27 – 25 – 16 – 8.
Resposta: GEOMETRIA


3. Bernardo codificou 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 codificou.
Resposta: 26 – 20 – 13 – 8 GATO
4. Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?
Resposta: Chave "avance 24 casas"

APÊNDICE Z: Atividade de Verificação – Experimentação

ATIVIDADE DE VERIFICAÇÃO – EXPERIMENTAÇÃO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

Nome do aluno(a): _____ Data: __/__/____

1) Questão (Fatec – 2017): Maria, aluna da Fatec Mococa, para garantir a segurança das mensagens que pretende transmitir, criou um sistema de criptografia da seguinte forma:

- montou uma tabela de 2 linhas e 13 colunas para colocar as 26 letras do alfabeto, sem repetição de letra;
- nas cinco células iniciais da 1ª linha, da esquerda para a direita, escreveu, uma a uma, as letras F, A, T, E, C nessa ordem;
- ainda na 1ª linha, na 6ª célula, da esquerda para a direita, obedecendo a ordem alfabética (de A a Z) colocou a primeira letra ainda não utilizada nas células anteriores;
- da 7ª célula a 13ª célula da 1ª linha, inseriu sete letras, da esquerda para a direita, sem repetir letra, seguindo a ordem alfabética, começando pela primeira letra ainda não utilizada nas células anteriores;
- preencheu a 2ª linha, da esquerda para a direita, com as letras restantes do alfabeto, também em ordem alfabética e sem repetição de qualquer letra já utilizada anteriormente.

A tabela mostra o início do processo, com as seis primeiras letras.

F	A	T	E	C	B							

Tendo construído a tabela conforme o descrito, para criptografar uma mensagem, Maria substitui cada letra da 1ª linha pela que está na 2ª linha, na mesma coluna, e vice-versa. A acentuação, a pontuação e o espaço entre as palavras são desconsiderados.

Assim, para desejar BOA PROVA para uma colega, que sabia fazer a decodificação, escreveu RTNEBTHN.

Para João, que também sabia decodificar a mensagem, Maria escreveu:

AGAQNENBPSPNEBPASPB

A partir da decodificação, João entendeu que a mensagem de Maria foi:

a) Nunca pare de aprender
b) Nunca deixe de estudar
c) Nunca faça isso de novo
d) Sempre tire boas notas
e) Sempre faça boas ações

2) Cifre a frase O SEGREDO NAO SERA REVELADO, utilizando a chave "avance 5 casas", e indique como a chave cifradora poderia ser escrita em linguagem matemática.

3) A palavra MATEMATICA foi cifrada por João utilizando uma chave cuja função decifradora $f: \mathbb{Z} \to \mathbb{Z}$ é definida por $f^{-1}(x) = x - 7$. Qual a função cifradora utilizada, e como ficou a mensagem?

4) Henrique recebeu uma carta misteriosa contendo a seguinte mensagem:

TUGFY GEHJHUGY YMYLRY.

E junto a mensagem havia três funções, das quais uma delas foi utilizada para cifrar a mensagem.

$$f(x) = x + 5$$

$$f(x) = -x + 26$$

$$f(x) = x - 4$$

Qual a mensagem original da carta?

APÊNDICE AA: Questionário Final – Experimentação

QUESTIONÁRIO II – EXPERIMENTAÇÃO

Prezado(a) aluno(a), esse instrumento é parte integrante de uma pesquisa promovida por Karina França Bragança, Ramon Chagas Santos e Silvana Leal da Silva, alunos do curso de Licenciatura em Matemática do IFFluminense – *campus* Campos Centro, sob orientação dos professores Lívia Azelman de Faria Abreu e Alex Cabral Barbosa. Sua participação é muito importante para esse trabalho, e sua identidade será preservada. Obrigado pela colaboração.

1- Nome do aluno(a): _____

2- Com base na escala abaixo:

D	Discordo
DP	Discordo parcialmente
NC/ND	Não Concordo e nem discordo
CP	Concordo parcialmente
C	Concordo

Em sua opinião, o estudo acerca do Tema Criptografia:

	D	DP	NC/ND	CP	C
Foi interessante.					
Agregou novo conhecimento.					
Apresentou relação com conteúdos Matemáticos.					
Foi apresentado de forma clara.					
Foi apresentado de forma atraente.					
Foi um estudo diferenciado.					

Contribuiu para o estudo da função inversa de uma função afim.					
Tornou o estudo da função inversa mais significativo com aplicação no cotidiano.					
Seria importante de ser abordado em sala de aula.					

O espaço a seguir é para comentários relacionados a qualquer afirmativa acima. Caso tenha assinalado a coluna D, DP ou NC/ND, mencione o(s) motivo(s) que levaram à essa(s) opção(ões).

3- Faça uma avaliação sobre o trabalho.