UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS PROF. DR. SÉRGIO JACINTHO LEONOR
MESTRADO PROFISSIONAL EM MATEMÁTICA

MOISÉS DE OLIVEIRA MOURA

A CRIPTOGRAFIA MOTIVANDO O ESTUDO DAS FUNÇÕES NO 9º ANO DO ENSINO FUNDAMENTAL

ARRAIAS-TO
2019

MOISÉS DE OLIVEIRA MOURA

A CRIPTOGRAFIA MOTIVANDO O ESTUDO DAS FUNÇÕES NO 9º ANO DO ENSINO FUNDAMENTAL

Dissertação apresentada ao Programa de Pós-Graduação em Matemática como requisito parcial à obtenção do grau de Mestre em Matemática.

Orientadora:
Profa. Dra. Keidna Cristiane Oliveira Souza

ARRAIAS-TO
2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

M929c Moura, Moisés de Oliveira.

A criptografia motivando o estudo das funções no 9º ano do Ensino Fundamental. / Moisés de Oliveira Moura. – Arraias, TO, 2019.

92 f.

Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Arraias - Curso de Pós-Graduação (Mestrado) Profissional em Matemática, 2019.

Orientadora : Dra. Keidna Cristiane Oliveira Souza

1. Criptografia e função afim. 2. A relação entre criptografia e funções. 3. A criptografia como motivação. 4. Codificando e decodificando com função afim. I. Título

CDD 510

MOISÉS DE OLIVEIRA MOURA[1]

A CRIPTOGRAFIA MOTIVANDO O ESTUDO DAS FUNÇÕES NO 9º ANO DO ENSINO FUNDAMENTAL

Dissertação apresentada ao Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede, foi avaliada para a obtenção do título de Mestre em Matemática, e aprovada em sua forma final pela Orientadora e pela Banca Examinadora.

Data de Aprovação: 03 / 05 / 2019

Banca Examinadora:

Profa. Dra. Keidna Cristiane Oliveira Souza, UFT
Orientadora

Prof. Dr. Bruno Trindade Reis, UFOB
Examinador

Profa. Dra. Alcione Marques Fernandes, UFT
Examinadora

Arraias - TO
2019

[1] O Autor foi bolsista CAPES.

Dedico este trabalho aos meus filhos Luís Felipe e Maria Eduarda, pela força que me deram e por sempre me dizer que sou capaz.

AGRADECIMENTOS

Gostaria de mencionar os meus sinceros agradecimentos a todos que de alguma forma contribuíram para que eu pudesse realizar e concluir essa etapa tão solene em minha vida.

Primeiramente agradeço a Deus por ter dado a força de que precisei para superar todos os obstáculos a minha frente, e também por ter oferecido as condições necessárias para que eu pudesse finalizar esse trabalho.

Agradeço aos meus filhos Maria Eduarda e Luís Felipe que sempre permaneceram ao meu lado e nunca duvidaram da minha capacidade.

Ao meu pai, que se aproxima do centenário e luta para não esquecer as lembranças devido à memória fraquejada e, mesmo assim, não se esquecia de perguntar se eu iria para Arraias na sexta-feira.

Agradeço aos meus irmãos e familiares, especialmente as minhas irmãs Cláudia e Rita, que me deram forças e sempre me ajudaram no que foi preciso.

Também agradeço à todos os amigos que conquistei durante a realização deste trabalho, especialmente aos meus amigos Frederico, Juliana e Luciano que estiveram presentes em todos os momentos e me ajudaram sempre que precisei.

Agradeço à professora Dr.^{a} Keidna, minha orientadora que, mesmo com todos os seus afazeres, se prontificou a me conduzir para que eu pudesse realizar esse trabalho.

Agradeço à UFT, campus de Arraias e aos professores do programa.

Agradeço à equipe diretiva e aos alunos do 9^o ano do Ensino Fundamental do Colégio Visão, em Formosa-Goiás, que colaboraram para a realização das atividades contidas neste trabalho.

Agradeço à SEEDF/EAPE, que me concedeu o afastamento remunerado para estudos, dando-me condições para fazer essa especialização com dedicação exclusiva.

Agradeço também à CAPES, pois me ajudou bastante ao conceder a bolsa de estudos.

Enfim, a todos aqueles que torceram por mim durante essa trajetória, meu muito obrigado.

RESUMO

A criptografia surgiu nos meios tecnológicos e de comunicação fazendo parte da realidade de nossos alunos, entretanto, parte dos educandos ainda a desconhece. Dessa forma, estabelecer uma conexão entre a criptografia contida neste contexto e os conteúdos vistos em sala de aula poderá proporcionar resultados positivos no âmbito escolar. Com isso em mente, o objetivo deste trabalho é apresentar a criptografia como uma ferramenta para contextualizar o conteúdo de funções, em particular, funções afins. Com o intuito de enriquecer o ensino da Matemática e despertar no educando o interesse pela Matemática, insere-se, então, a criptografia ao conteúdo das funções afins no 9º ano do Ensino Fundamental. Associar o ensino de funções à criptografia é um meio de informar ao discente de que tudo aquilo que ele estudou até então, por mais básico que seja, é aplicável e útil, neste caso essencial, para o desenvolvimento seguro da tecnologia. Para o desenvolvimento do trabalho, foi estabelecida uma estratégia, com os alunos, iniciada com um pré-teste com o objetivo de verificar seus conhecimentos em relação ao tema abordado; depois, foram levantados os aspectos históricos tanto de criptografia quanto de funções e, finalmente, fez-se a conexão entre os dois temas, totalizando 6(seis) encontros. Os dados foram coletados mediante pré-teste, pós-teste e respostas às atividades. Além disso, foi feito um estudo bibliográfico, o que confere à pesquisa um caráter qualitativo e visa facilitar a compreensão do conteúdo das funções afins, por meio da contextualização proporcionada pela relação estabelecida entre a criptografia e funções.

Palavras-chave: Criptografia. Funções. Motivação. Intervenção.

ABSTRACT

The cryptography arises in the technological and communication media as part of the reality of our students, however, some of the students still do not know this. In this way, establishing a connection between the cryptography contained in this context and the content seen in the classroom can generate positive results in the school environment. With this in mind, the purpose of this work is to present the cryptography as a tool to contextualize the content of functions, in particular, the affine functions. With the intention of enriching the teaching of Mathematics and awakening in the student the interest in Mathematics, the cryptography was added to the content of the functions affine to the 9th year of Elementary School. Relating the teaching of functions to cryptography is a way of informing him that everything he has studied up to then, however basic, is applicable and useful, in this essential case, to the safe development of technology. For the development of the work, a strategy was established with the students, started with a pre-test with the objective of verifying their knowledge in relation to the topic addressed; Then, historical aspects of cryptography and functions were raised, and finally, the connection between the two themes was made, totaling 6 (six) encounters. Data were collected through pre-test, post-test and responses to activities. In addition, a bibliographic study was carried out, which gives the research a qualitative character and aims to facilitate the understanding of the content of the affine functions, through the contextualization provided by the relation established between the cryptography and the functions.

Key-words: Cryptography. Functions. Motivation. Intervention.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BNCC	Base Nacional Comum Curricular
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
DES	Data Encryption Standard (Padrão de Criptografia de Dados)
EAPE	Escola de Aperfeiçoamento dos Profissionais da Educação
IDEA	International Data Encryption Algorithm (Algoritmo Internacional de Criptografia de dados)
IMPA	Instituto de Matemática Pura e Aplicada
MIT	Massachusetts Institute of Technology (Instituto de Tecnologia de Massachusetts)
OBMEP	Olimpíada Brasileira de Matemática das Escolas Públicas
PCN	Parâmetros Curriculares Nacionais
PROFMAT	Mestrado Profissional em Matemática
RC	Ron's Code ou Rivest Cipher (Código de Ron ou Cifra de Rivest)
RSA	Rivest, Shamir and Adleman (Iniciais dos sobrenomes dos três autores)
SEEDF	Secretaria de Estado de Educação do Distrito Federal
UFPE	Universidade Federal de Pernambuco

SUMÁRIO

1 INTRODUÇÃO

Devido ao avanço tecnológico dos meios de comunicação de última geração, como smartphones, computadores, tablets, internet, satélites e outros, houve uma mudança comportamental das pessoas em nossa sociedade. Atualmente, boa parte das pessoas utilizam-se desse avanço tecnológico, ficando diariamente conectadas em redes sociais, aplicativos de bate-papo, jogos on-line, compartilhando arquivos e realizando algum tipo de transação financeira. Porém, para essa comodidade, existe um risco, pois as informações enviadas e recebidas por esses equipamentos trafegam livremente a todo o momento. Isto posto, essas informações devem ser protegidas para evitar que terceiros tenham acesso a elas e, consequentemente, possam causar algum tipo de transtorno.

Neste cenário, a criptografia garante a manutenção desses meios de comunicação, uma vez que sua função é promover a segurança do sistema e de seus usuários.

Assim, surge a ideia de relacionar o tema criptografia com o conteúdo de funções, aproximando, dessa forma, o cotidiano do aluno ao conteúdo científico visto em sala de aula. Além de sua importância na segurança de informações, a criptografia estabelece conexões com diferentes temas da Matemática, logo, existem aplicações em diversas áreas e níveis do conhecimento, tornando-a, assim, uma ferramenta motivadora para o estudo de funções.

O objetivo deste trabalho é apresentar a criptografia como uma ferramenta para contextualizar o conteúdo de funções, em particular, funções afins.

A metodologia utilizada no trabalho envolve um estudo bibliográfico e também uma pesquisa de caráter qualitativo que teve como instrumentos de coleta de dados a observação direta, pré-teste, pós-teste e respostas das atividades propostas. As atividades foram desenvolvidas com alunos do 9^o ano do Ensino Fundamental do Colégio Visão, na cidade de Formosa-Goiás. Ao todo, foram envolvidos dezesseis alunos, dos quais, seis do sexo masculino e dez do sexo feminino, na faixa etária entre treze e quatorze anos.

Durante a pesquisa bibliográfica para desenvolvimento deste trabalho, um questionamento nos foi levantado: Quais são as aplicações de conceitos da criptografia no processo de aprendizagem da função afim? A hipótese é que o ensino do conteúdo de criptografia tenha uma relação direta com o estímulo no estudo da função afim.

Atuando como professor da Educação Básica, há mais de 20 anos na disciplina de Matemática no Distrito Federal e Goiás, venho percebendo, ao longo desse período, a falta de interesse ou motivação por parte de alguns alunos em relação a essa disciplina. Os relatos frequentes, apontados por eles, são: resoluções excessivas de exercícios, aulas cansativas e o porquê aprender esses conteúdos, já que a maioria deles não será utilizado em seu cotidiano.

Esta dissertação surgiu com a idealização de relacionar situações recorrentes aos alunos com os conceitos matemáticos trabalhados em sala de aula e também causar efeito na prática didática, contemplando, assim, o regimento do Mestrado Profissional em Matemática – PROFMAT. Desse modo, espera-se que a criptografia, ao ser inserida ao conteúdo de funções, produza um efeito motivador, uma vez que o aluno percebe que existe uma relação entre sua rotina e o que se aprende em sala de aula.

Esta dissertação estrutura-se em seis capítulos, dispostos na seguinte sequência: no primeiro capítulo, apresentamos a Introdução.

No segundo capítulo, apresentamos uma contextualização histórica sobre a criptografia, cuja intenção é elucidar seu desenvolvimento e sua importância ao longo da história.

No terceiro capítulo, embasado em pesquisas bibliográficas, abordamos uma síntese sobre a evolução do conceito de função e também apresentamos as definições das funções afim, injetora, sobrejetora, bijetora e da função inversa, uma vez que estes conceitos e definições são essenciais para que o aluno possa compreender e aplicar a relação entre criptografia e função.

No quarto capítulo, estabelecemos a conexão entre criptografia e funções e também fazemos uma análise de trabalhos similares para fortalecer ainda mais o objetivo da pesquisa.

No capítulo cinco, apresentamos a proposta do trabalho bem como todos os procedimentos para que o objetivo fosse alcançado. Nesse capítulo, apresentamos a estratégia e mostramos todas as etapas de realização e conclusão do trabalho. A estratégia consistia em uma explanação do tema da pesquisa e aplicações de pré-teste e pós-teste aos alunos do 9º ano do Ensino Fundamental do Colégio Visão, um colégio da rede Privada de Ensino, na cidade de Formosa-Goiás. Esses pré-teste e pós-teste tinham a finalidade de comparar e analisar os dados coletados para verificar se o objetivo foi alcançado.

No sexto e último capítulo, apresentamos as Considerações Finais. E desse modo, o que percebemos é que, por meio da conexão estabelecida entre criptografia e funções, ocorreram mudanças positivas, relacionadas ao empenho e participação dos estudantes envolvidos nesse processo.

2 CRIPTOGRAFIA - CONTEXTO HISTÓRICO

Ao longo da história, o homem esteve à procura de novos horizontes, fundou civilizações e buscou aprimorar seus conhecimentos. A escrita foi um dos pilares no progresso de suas civilizações e, com o passar dos séculos, surgiu a necessidade de se comunicar através de mensagens. Com o propósito de obter a segurança do conteúdo dessas mensagens, técnicas foram criadas e aperfeiçoadas, para ocultar o seu verdadeiro sentido. Se por um lado existiu a preocupação em manter o sigilo de suas comunicações, por outro lado, houve o interesse em desvendar seus segredos, surgindo, assim, a criptologia.

Para Kahn (1973),

> Criptologia é, por definição, uma atividade social, sendo assim pode ser examinada de um ponto de vista sociológico. Se trata de comunicação sigilosa, e a comunicação talvez seja a mais complexa e variada atividade humana. Engloba não somente palavras, mas gestos, expressões faciais, tons de voz e até mesmo o silêncio (KAHN, 1973, p. 447, tradução nossa).

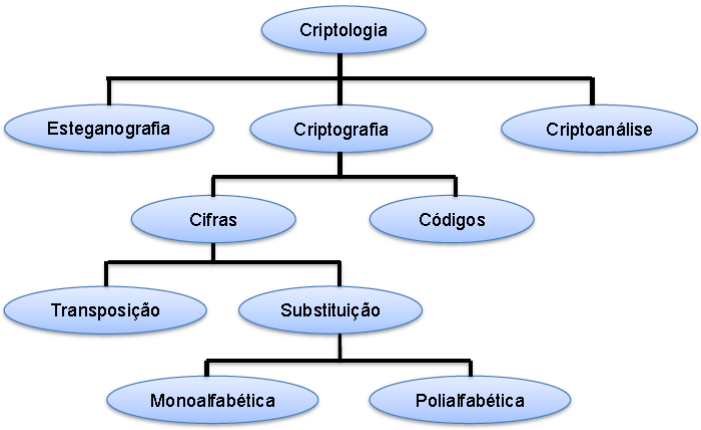
Bezerra; Malagutti e Rodrigues (2010, p. 3) diz que "A criptologia é a ciência que se ocupa da ocultação de informações (criptografia) e da quebra das informações ocultadas (criptoanálise)."

Uma informação pode ser escondida de duas maneiras diferentes:

- Ocultando a existência da mensagem (esteganografia).
- Ocultando o significado do conteúdo da mensagem (criptografia).

Abaixo, temos um diagrama da criptologia e suas ramificações.

Figura 1 – Diagrama da criptologia e suas ramificações



Fonte: Bezerra; Malagutti e Rodrigues (2010)

Neste capítulo, faremos uma breve contextualização histórica da evolução da criptografia. No entanto, é bom ressaltar que existem vários episódios na história em que aparece a criptografia, porém destacaremos apenas alguns desses acontecimentos.

Daremos início, fazendo menção ao bastão de Licurgo e chegaremos aos dias de hoje, expondo a importância do sistema RSA. Finalmente, finalizaremos a contextualização, falando sobre o misterioso manuscrito de Voynich. Inicialmente, a criptografia teve seu ápice nos segredos militares, tendo papel substancial nas decisões de batalhas e segredos de Estado. Atualmente, ela se destaca em garantir a segurança de nossas informações na *web* e manter a privacidade dos usuários na Era da Informação.

2.1 O bastão de Licurgo

O bastão de Licurgo, também conhecido como *scytale* ou *citale* espartano, é a cifra de transposição mais antiga. "Uma cifra de transposição é aquela em que cada letra de uma mensagem muda sua posição dentro do texto, mas retém sua identidade" (SINGH, 2004, p. 422). Essa técnica foi utilizada por volta de 475 a.C., tornando-se o primeiro aparelho criptográfico militar.

> No ano 404 a.C., Lisandro de Esparta recebeu um mensageiro ensanguentado e ferido, único sobrevivente de um grupo de cinco que partira da Pérsia numa árdua jornada. O mensageiro lhe entregou seu cinturão, que Lisandro enrolou em torno de seu *citale* para descobrir que o persa Farnabazo estava planejando atacá-lo. Graças ao *citale*, Lisandro estava preparado para o ataque, e o repeliu (SINGH, 2004, p. 25).

Esse sistema criptográfico consiste em um bastão de madeira ao qual era enrolada, ao seu redor, uma tira de couro ou pergaminho. Nessa tira, a mensagem deveria ser escrita no sentido do comprimento do bastão e, depois, bastaria desenrolar a tira, para obter o conteúdo da mensagem cifrada.

Figura 2 – Bastão de Licurgo

Fonte: Medeiros (2013)

O receptor da tira precisaria ter um bastão idêntico para que a mensagem pudesse ser lida. "Cifrar uma mensagem é qualquer sistema em geral para esconder o significado de uma mensagem substituindo cada letra da mensagem original por outra letra". (SINGH, 2004, p. 422). O algoritmo da cifra, neste caso, é o enrolar da tira no bastão e a chave, a sua largura.

> Algoritmo de cifragem é qualquer processo geral de cifragem que pode ser especificado, exatamente, pela escolha de uma chave. A chave é o elemento que transforma o algoritmo de cifragem geral num método específico de cifragem. De um modo geral, o inimigo pode saber qual é

> o algoritmo de cifragem sendo usado pelo remetente e o destinatário da mensagem, mas ele não pode conhecer a chave (SINGH, 2004, p. 421).

Segundo Medeiros (2013), uma maneira de visualizar a distribuição de uma mensagem é transpô-la para uma tabela. Para isso, dividimos o total de caracteres da mensagem pelo número de linhas (o que equivale a sua largura) e obtemos o número de colunas da tabela. Por exemplo, tomemos a célebre frase de Albert Einstein: "**A matemática não mente. Mente quem faz mau uso dela**". Agora, devemos escrever a mensagem sem espaços, pontos ou acentos e teremos a seguinte mensagem a ser cifrada: **"amatematicanaomentementequemfazmauusodela"**.

Neste exemplo, utilizou-se um bastão de madeira (pedaço de um cabo de rodo ou vassoura) com 30 cm de comprimento e 6,0 cm de largura. A tira utilizada para escrever a mensagem foi uma tira de papel com 60 cm de comprimento por 1,5 cm de largura.

Para construir a tabela, dividiremos os 41 caracteres dessa mensagem por 6, que corresponde a largura do bastão (chave) 6, obtendo assim, um valor aproximado de 7 colunas. Como a divisão não é inteira, o último espaço na tabela ficará sem ser preenchido. Assim, escreveremos a frase a ser cifrada na tabela, da esquerda para a direita e de cima para baixo, assim:

Tabela 1 – Método para visualizar a distribuição de uma mensagem

a	m	a	t	e	m	a
t	i	c	a	n	a	o
m	e	n	t	e	m	e
n	t	e	q	u	e	m
f	a	z	m	a	u	u
s	o	d	e	l	a	

Fonte: Autor

Para obter a cifragem, devemos escrever a mensagem de cima para baixo e da esquerda para a direita. Assim, o texto cifrado será:

ATMNFSMIETAOACNEZDTATQMEENEUALMAMEUAAOEMU

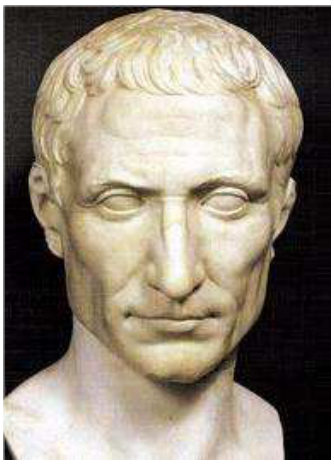
Para ler o conteúdo da frase, basta enrolar a tira em outro bastão idêntico ao bastão anterior.

2.2 A cifra de César

Segundo Singh (2004), o líder militar e governante romano, Caio Júlio César (100 a.C. – 44 a.C.) teve um papel fundamental na passagem da República para o Império

Romano. Durante o seu governo, fez grandes conquistas militares para Roma, que se estenderam da Gália até o oceano Atlântico. Em função de suas habilidades militares, César teve uma preocupação em relação à segurança de suas informações. Pensando nisso, ele desenvolveu um sistema que garantia a segurança de suas mensagens caso fossem interceptadas pelo inimigo. Esse sistema ficou conhecido como *código de César* ou *cifra de César*.

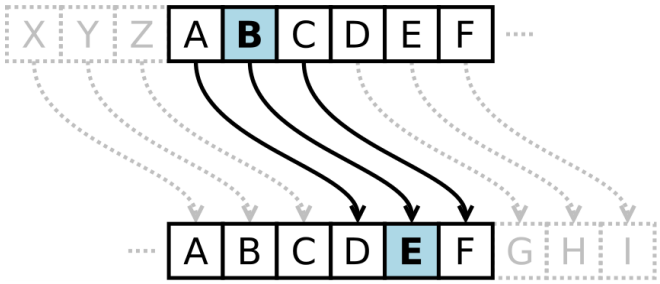
Figura 3 – Júlio César de Roma



Fonte: Pereira (2015)

Esse código era um sistema simples de substituição, no qual cada letra da mensagem original era substituída pela letra que se situa três posições a sua frente. Assim, como mostrado na figura 4, a letra A era substituída pela letra D, a letra B era substituída pela letra E, e assim sucessivamente.

Figura 4 – Deslocamento utilizado por Júlio César



Fonte: Pereira (2015)

A transformação pode ser representada alinhando-se dois alfabetos; o alfabeto normal e o alfabeto cifrado, obtido deslocando três casas em relação ao alfabeto normal.

Alfabeto normal 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

Alfabeto cifrado 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

Para fazer a codificação de uma mensagem, deve-se simplesmente observar cada letra da mensagem no texto "normal"e escrever a letra correspondente na linha "cifrada". Para fazer a decodificação, deve-se fazer o processo contrário.

> Codificar é passar um texto simples por transformações, isso é codificar, conforme o caso. O que sai dessa transformação é o texto cifrado, a mensagem secreta. Decifrar ou decodificar é para as pessoas que legitimamente possuem a chave e o método para reverter as transformações e descobrir a mensagem original (KAHN, 1973, p. 6, tradução nossa).

Vejamos, como exemplo, a frase de Carl Friedrich Gauss:

Texto normal **"a matemática é a rainha das ciências"**.

Texto cifrado **D PDWHPDWLFD H D UDLQKD GDV FLHQFLDV**.

Este sistema de substituição foi usado pela primeira vez com a finalidade militar, por Júlio César, nas guerras da Gália. César relata a mensagem que enviou a Cícero que se encontrava à beira da rendição.

> O mensageiro recebeu instruções para que, se não pudesse se aproximar, jogasse uma lança com a mensagem amarrada por uma tira de couro, dentro das fortificações do campo... Com medo, o gaulês arremessou a lança como fora instruído. Por acaso, a arma encravou-se em uma torre e passou dois dias sem ser vista pelos nossos soldados, até que, no terceiro dia, ele a leu e depois a recitou em voz alta à tropa em formação, trazendo grande alegria para todos (SINGH, 2004, p. 26).

Se uma codificação usar a cifra de substituição de César, potencialmente poderá ser decifrada sem grandes esforços, pois esse tipo de codificação possui um total de 25 chaves em potencial, já que existem apenas 25 deslocamentos possíveis. Por outro lado, se não limitarmos a mover as casas ordenadamente, então teremos uma permutação de 26 elementos (devido à nova reforma ortográfica, o nosso alfabeto agora se compõe de 26 letras). Assim, será inviável ao inimigo tentar decifrá-la, já que existem aproximadamente 400.000.000.000.000.000.000.000.000 de chaves diferentes.

2.3 Maria Stuart, rainha da Escócia, o poder de um código

De acordo com Singh (2004), em 1542, uma semana após seu nascimento no palácio de Linlithgow, Maria perde seu pai, Jaime V, rei da Escócia. Aos seis anos, no dia 7 de agosto de 1548, ela foi enviada a França para sua própria segurança, devido aos conflitos constantes liderados pelos ingleses. Aos dezesseis anos de idade, casou-se com o herdeiro do trono francês, Francisco II e, dois anos depois, em 1561, Maria retorna viúva a sua terra natal. Ao chegar à Escócia para assumir o trono, encontrou seu país bem diferente daquele que ela havia deixado. Sua fé católica não agradava os escoceses,

voltados cada vez mais para a Igreja Protestante, e muito menos, a própria Inglaterra. Mais tarde, em 1565, com 23 anos de idade, Maria se casa novamente, agora com seu primo Henrique Stuart, o conde de Darnley, conhecido por seu caráter perverso, bárbaro e ambicioso, o que culminou em uma ofensiva para retirá-lo do poder e, após tentativa de fuga, foi estrangulado e sua casa destruída. Os nobres escoceses, insatisfeitos com sua rainha, resolveram exilar James Hepburn, o conde de Bothwell, seu terceiro marido e condená-la à prisão, forçando-a a abdicar de seu trono em favor de seu filho.

Ao fugir da prisão, Maria se dirigiu para a Inglaterra, esperando que sua prima, a rainha Elizabeth I, lhe desse refúgio, porém foi surpreendida com uma nova prisão. Na Inglaterra, Maria era considerada uma ameaça, pois Elizabeth era protestante e os nobres católicos ingleses acreditavam na legitimidade de Maria em substituir Elizabeth no trono inglês. Assim permaneceu encarcerada por mais 18 anos. Em 1586, não tendo mais os seus privilégios e totalmente sem esperanças, sem que Maria soubesse, o jovem Anthony Babington[1], de 24 anos, juntamente com outros católicos, arquitetaram um plano para salvá-la e por fim ao reinado de sua prima, a rainha Elizabeth.

Figura 5 – Maria Stuart

Fonte: Singh (2004)

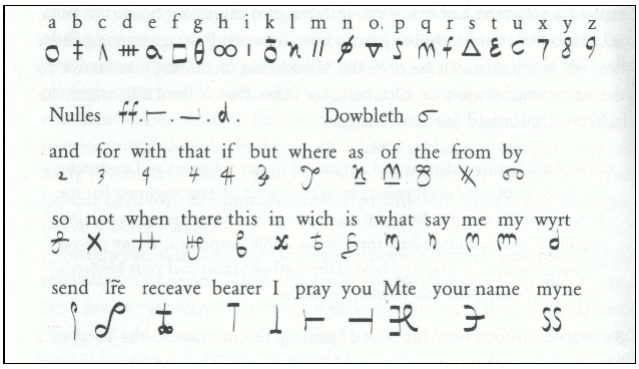
A conspiração ficou conhecida como o plano de Babington e, para poder articular o esquema sem que os ingleses soubessem, era colocada uma mensagem cifrada dentro de um saco de couro, em uma tampa oca de um barril de cerveja. A mensagem era cifrada, pois, se ela fosse interceptada pelo carcereiro de Maria, ninguém poderia conhecer o seu conteúdo.

[1] Anthony Babington (1561 - 1586) foi um nobre inglês condenado por tramar o assassinato da rainha Elizabeth I da Inglaterra e de conspirar com a prisão de Maria Stuart. Foi executado em 20 de setembro de 1586.

> Como precaução extra, Babington cifrou a carta, de modo que, mesmo que fosse interceptada pelo carcereiro de Maria, ela seria indecifrável e o complô não seria descoberto. Ele usou uma cifra que não era uma simples substituição monoalfabética e sim um nomenclador [...]. Consistia em 23 símbolos que deviam substituir as letras do alfabeto (excluindo j, v e w), junto com 36 símbolos representando palavras e frases. Além disso, havia quatro símbolos nulos e o símbolo σ significando que o símbolo seguinte representava uma letra dupla (SINGH, 2004, p. 54).

A figura 6 mostra o nomenclador de Maria, rainha da Escócia, consistindo em um alfabeto cifrado e uma palavra-código.

Figura 6 – Nomenclador de Maria



Fonte: Jasper (2009)

O que eles não contavam é que um de seus ajudantes, Gilbert Gifford, era um agente duplo que oferecera seus serviços à Sir Francis Walsingham, primeiro-secretário da rainha Elizabeth, implacável, um mestre da espionagem e responsável pela sua segurança. Thomas Phelippes, secretário de cifras de Walsingham e um mestre da análise de frequência, decifrou a mensagem de Babington para Maria, propondo o assassinato da rainha Elizabeth. Dessa forma, não existia mais nenhuma dúvida quanto ao seu envolvimento no complô. Assim, no dia 8 de fevereiro de 1587, no Grande Salão do Castelo de Fotheringhay, Maria, a rainha da Escócia foi condenada e sua sentença foi a decapitação. A história de Maria Stuart evidencia a importância da criptografia e como ela foi decisiva em seu julgamento.

2.4 A cifra de Vigenère

Após o surgimento da análise de frequência no mundo árabe, técnica que permite decifrar uma mensagem sem conhecer a chave, percebe-se a vulnerabilidade da cifra de substituição monoalfabética, um exemplo foi a execução de Maria, rainha da Escócia.

> Embora não se saiba quem percebeu em primeiro lugar que as frequências das letras podiam ser exploradas de modo a quebrar códigos, a mais antiga descrição conhecida desta técnica nos vem de um cientista do século IX, Abu Yusef Ya' qub ibn Is-haq ibn as-Sabbah ibn omran

> ibn Ismail al-Kindi. Conhecido como "o filólosofo dos árabes" (SINGH, 2004, p. 33).

Frente à fragilidade da cifra de substituição monoalfabética, os criptógrafos "pessoa especializada em desenvolver novos métodos de escrita secreta" (SINGH, 2004, p. 32) perceberam a necessidade de criar uma nova cifra, mais forte e que pudesse vencer os criptoanalistas "pessoa que luta para encontrar fraquezas nesses métodos, de modo a quebrar a mensagem secreta." (SINGH, 2004, p. 32). A ideia seria utilizar em conjunto vários alfabetos, ou seja, um sistema de substituição polialfabética. Abaixo, David Kahn, em seu livro *The Codebreakers*, faz uma definição desses sistemas.

> Enquanto apenas uma cifra alfábetica esta em uso, o sistema é chamado monoalfabético. Quando, no entanto, duas ou mais cifras alfabéticas são utilizadas em um tipo de padrão pré-estabelecido, o sistema se torna polialfabético (KAHN, 1973, p. 4, tradução nossa).

Segundo Singh (2004), tudo começou com Leon Battista Alberti, considerado um dos mais importantes representantes da arquitetura renascentista italiana do século XV. Ele propôs o uso de dois ou mais alfabetos cifrados, usados alternadamente. Segundo ele, seria mais fácil confundir os criptoanalistas em potencial. Essa ideia foi sendo aperfeiçoada posteriormente por Johannes Trithemius, logo depois por Giovanni Porta e finalmente pelo diplomata francês Blaise de Vigenère.

Figura 7 – Blaise de Vigenère

Singh (2004)

Dispondo do conhecimento desses trabalhos e após examiná-los minuciosamente, Vigenère pode elaborar uma nova cifra imune à análise de frequência. A cifra de Vigenère faz parte de uma classe conhecida como *cifra polialfabética* e consiste na sequência de várias *cifras de César* com diferentes valores de deslocamentos, como mostrado na figura 8 a seguir:

Figura 8 – O quadro de Vigenère

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	w	v	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	W	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	W	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
22	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	W
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	W	V
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X	Y	Z

Fonte: Ferroni (2002)

Para cifrar a mensagem: **"Zero, esse nada que é tudo"**, frase dita pelo matemático Charles-Ange Laisant, usando a cifra de Vigenère, devemos proceder da seguinte maneira. Primeiro devemos escolher uma palavra chave, por exemplo: PROFMAT e escrevê-la repetidamente até completar todos os caracteres da mensagem, veja tabela 2 a seguir:

Tabela 2 – Distribuição da palavra-chave PROFMAT com as letras da mensagem

Palavra chave	P	R	O	F	M	A	T	P	R	O	F	M	A	T	P	R	O	F	M	A
Mensagem	z	e	r	o	e	s	s	e	n	a	d	a	q	u	e	e	t	u	d	o

Fonte: Autor

Para cifrar as letras da mensagem, é necessário usar a linha do quadro de Vigenère correspondente à letra da palavra-chave relacionada. Então, para cifrar a letra z, devemos escolher a letra da palavra-chave que corresponde a esse z, no caso P, e no quadro de vigenère, a letra P representa a 15^a linha. Daí, a letra z será cifrada pela letra O. Fazendo esse procedimento com o restante das letras da mensagem, encontramos a mensagem cifrada conforme tabela 3.

Tabela 3 – Letras cifradas usando o quadro de Vigenère com a palavra-chave

Pal. chav.	P	R	O	F	M	A	T	P	R	O	F	M	A	T	P	R	O	F	M	A
Mensagem	z	e	r	o	e	s	s	e	n	a	d	a	q	u	e	e	t	u	d	o
Mens. cif.	O	W	F	T	Q	S	L	T	E	O	I	M	Q	N	T	W	H	Z	P	O

Fonte: Autor

Mensagem cifrada: **OWFTQSLTEOIMQNTWHZPO**

Observando a tabela 3, podemos notar que a cifra de Vigenère, envolve diferentes valores de deslocamento. Nesse exemplo, a letra "z" desloca 15 casas para ser cifrada pela letra "O", a letra "o" desloca 5 casas para ser cifrada pela letra "T" e a letra "e" desloca 17 casas para ser cifrada pela letra "W" e 12 casas para ser cifrada pela letra "Q", em função da palavra-chave PROFMAT.

Apesar de a cifra de Vigenère ser imune à análise de frequência, sua aceitação não teve o merecido reconhecimento devido à dificuldade em manuseá-la.

2.5 A Enigma

Segundo Singh (2004), inspirado no desfecho do telegrama Zimmermann na Primeira Guerra Mundial (1914 – 1918), o alemão, Arthur Scherbius, pretendia substituir os sistemas de criptografia inadequados, usados nesse período. Esses sistemas ainda usavam cifras feitas no papel e lápis e ele pretendia substituí-los por um sistema de cifragem mais moderno e eficiente. Seu sistema de cifragem era semelhante à primeira máquina criptográfica desenvolvida por Leon Alberti, no século XV, porém desenvolvido com a tecnologia moderna do século XX.

> O telegrama Zimmermann foi um telegrama codificado despachado pelo ministro do exterior do Império Alemão, Arthur Zimmermann, em 16 de janeiro de 1917, para o embaixador alemão no México, Heinrich von Eckardt, no auge da Primeira Guerra Mundial. O embaixador era instruído a se aproximar do governo mexicano, com a proposta de formar uma aliança militar contra os Estados Unidos. A proposta promete ao México terras dos Estados Unidos caso o país aceitasse o acordo. O telegrama foi interceptado e decodificado por britânicos e seu conteúdo apressou a entrada dos Estados Unidos na Primeira Guerra Mundial (KRISCHER, 2013, p. 97).

Depois de vários anos melhorando sua invenção, "Em 1925, Scherbius começou a produção em massa de máquinas Enigma, que passaram a ser usadas pelos militares no ano seguinte" (SINGH, 2004, p. 161). A figura 9 mostra uma máquina Enigma usada pelo exército alemão. Posteriormente, elas foram adotadas pelo governo e pelas empresas estatais, como ferrovias.

Figura 9 – Uma máquina Enigma usada pelo exército alemão com a tampa interna aberta, revelando seus componentes.

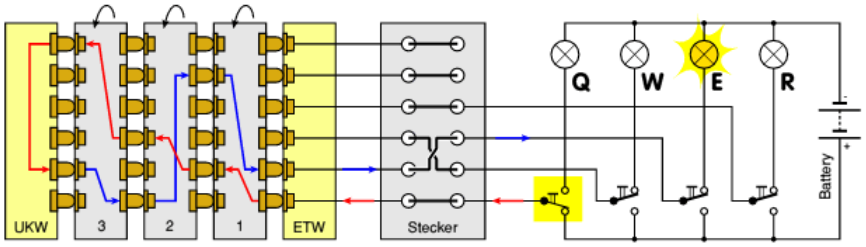
Fonte: Singh (2004)

Nas duas décadas seguintes, os militares alemães compraram 30 mil máquinas Enigma. E a invenção de Scherbius deu aos alemães o sistema mais seguro de criptografia do mundo.

> A forma básica da invenção de Scherbius consiste em três elementos conectados por fios: um teclado para a entrada de cada letra do texto original, uma unidade misturadora, que cifra cada letra, transformando-a na letra correspondente da mensagem cifrada, e um mostrador consistindo em várias lâmpadas para indicar as letras do texto cifrado (SINGH, 2004, p. 146).

A figura 10 mostra o diagrama de circuito de uma máquina Enigma padrão, mostrando o funcionamento de uma máquina Enigma I, utilizada pelo exército alemão durante a Segunda Guerra Mundial (1939 – 1945).

Figura 10 – Circuito com 3 rotores, 1 refletor de corrente (UKW) e 1 misturador no painel de plugues (ETW)



Fonte: Crypto (2008)

Para evitar um padrão de cifragem, Arthur Scherbius introduziu mais dois discos misturadores. Portanto, para cada um dos três misturadores em um alfabeto de 26 letras, podem ser ajustadas 26 orientações diferentes, fornecendo um total de 26 x 26 x 26, ou seja, 17.576 ajustes diferentes. Além disso, ele também desenvolveu um sistema de troca entre os três misturadores (uma permutação simples entre eles), dando a Enigma mais seis modos diferentes de se disporem os três misturadores (123, 132, 213, 231, 312, 321). Finalmente, ele inseriu um painel de tomadas entre o teclado e o primeiro misturador; dessa maneira, o número de modos de se conectar e, portanto, trocar seis pares de letras escolhidos entre as 26 letras, é bastante elevado: 100.391.791.500.

> O misturador, um espesso disco de borracha cheio de fios, é a parte mais importante da máquina. Partindo do teclado, os fios entram no misturador em seis pontos diferentes e fazem uma série de voltas e torções dentro do misturador antes de emergirem de outros seis pontos no lado oposto (SINGH, 2004, p. 146).

Sendo assim, o número total de chaves possíveis corresponde ao produto desses três resultados obtidos: 17.576 x 6 x 100.391.791.500 = 10.000.000.000.000.000. É bom

salientar que, ao resultado obtido, não foi incluído o efeito dos anéis[2]. Portanto, o número de chaves possíveis é ainda maior e as chances de decifrar uma mensagem da máquina Enigma são cada vez menores.

Em seu livro *O livro dos códigos*, Singh (2004) diz que em 1926, após admitir o fracasso de seus sistemas criptográficos na Primeira Guerra Mundial, o exército alemão passou a adotar a Enigma em suas operações militares e concluíram que a máquina Enigma seria a melhor opção para manter o sigilo de suas comunicações.

Figura 11 – Veículo de comando do general Heinz Guderian.[3] Uma máquina Enigma pode ser vista em uso no canto inferior esquerdo da foto

Fonte: Singh (2004)

Durante a Segunda Guerra Mundial, a Enigma se tornou o sistema de criptografia mais importante e seguro já conhecido. Os alemães tinham tanta confiança no sistema, que acreditavam que ele jamais poderia ser decifrado, graças a seus três diferentes rotores[4] de substituição polialfabética, que alcançavam 159 trilhões de combinações diferentes.

Em virtude da busca incansável para decifrar as mensagens alemãs, enviadas pela máquina Enigma durante a Segunda Guerra Mundial. Um verdadeiro exército foi reunido, composto por intelectuais e professores das universidades de Oxford e Cambridge, entre eles: Alan Mathison Turing (1912 – 1954), considerado o pai da ciência computacional, Peter Frank George Twinn (1916 – 2004) e Alfred Dilly Knox (1884 – 1943), decifradores de códigos. Seus trabalhos e esforços tiveram papel fundamental para a vitória dos aliados,

[2] O anel é o componente responsável pelo avanço do rotor e contém, na sua superfície exterior, os números de 01 a 26, ou as letras de A a Z. Em particular, a posição destes anéis relativamente ao cilindro central do rotor é também um dos elementos da chave que é necessário saber para decifrar uma mensagem. (Informações sobre o anel pode ser consultado no livro *The Codebreakers* de David Kahn).

[3] Heinz Wilhelm Guderian foi teórico militar e inovador general do exército alemão durante a Segunda Guerra Mundial

[4] Rotores é o conjunto de discos rotativos dispostos em fila na máquina Enigma e sua função é embaralhar os caracteres da mensagem.

pois, graças às mensagens decifradas e, consequentemente, dando a eles a localização de navios inimigos, os aliados venceram a Batalha do Atlântico, afundando muitos submarinos alemães. O Enigma teve uma contribuição fundamental no desenvolvimento de novas tecnologias, pois a busca em decifrar as mensagens enviadas por esse sistema contribuiu para o surgimento dos primeiros computadores.

2.6 O sistema RSA

Existem inúmeros algoritmos que realizam a criptografia para tentar esconder os dados de um acesso público. Nesse processo, são usados dois tipos de chaves para criptografar uma mensagem: simétricas e assimétricas. Nos processos que envolvem as chaves simétricas, a mesma chave é utilizada tanto pelo emissor quanto por quem recebe a informação, ou seja, é utilizada para codificar e para a decodificação dos dados, temos, por exemplo: O Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Ron's Code ou Rivest Cipher (RC) e o Blowfish.

As chaves assimétricas trabalham com duas chaves: uma privada e outra pública. A chave pública é de livre acesso, ou seja, qualquer pessoa poderá usá-la para criptografar uma mensagem. No entanto, para desfazer a criptografia, é necessário o uso da chave privada, cujo conhecimento pertence apenas o destinatário da mensagem.

> Uma das chaves serve para cifrar mensagens e pode ser divulgada livremente – todos têm acesso a ela – por isto mesmo é chamada como chave pública. Por outro lado, para decifrar mensagens, há a necessidade de uma chave secreta, conhecida apenas pelo indivíduo para o qual a mensagem foi enviada. Por isto, esta chave é conhecida como chave secreta (BEZERRA; MALAGUTTI; RODRIGUES, 2010, p. 108).

O El Gamal e o Rivest, Shamir and Adleman (RSA) são exemplos de chaves assimétricas. O RSA é um dos algoritmos mais usados e bem-sucedidos atualmente.

> Foram Ronald Rivest, Adi Shamir e Leonard Adleman, do Laboratório de Ciências da Informação do Massachusetts Institute of Technology (MIT), que deram em 1978 o passo decisivo para a implementação do primeiro sistema criptográfico com chaves assimétricas, idealizado por Driffie. O princípio baseia-se na relativa facilidade de encontrar números primos grandes e ao mesmo tempo na enorme dificuldade prática em fatorar o produto de dois desses números, além do uso de propriedades relativamente elementares da Teoria dos Números (HEFEZ, 2014, p. 319-320).

Fatorar números pequenos é algo simples, mas fatorar números grandes é bem difícil e demorado. Essa propriedade é que garante a segurança do RSA.

Em *Aprendendo Criptologia de Forma Divertida*, Bezerra, Malagutti e Rodrigues (2010), explicam o funcionamento do sistema RSA de uma forma bem simples. A estratégia

será transformar letras em números e construir uma função bijetora $f(x)$ que será usada para fazer a codificação de mensagens. Para decifrar as mensagens, usaremos a função $h(x)$, inversa de $f(x)$. De certa maneira, quanto mais fácil obtermos a inversa $h(x)$ de $f(x)$, mais fácil será quebrar o código, ou seja, mais frágil será o método de criptografia empregado.

Para obter as funções $f(x)$ e $h(x)$ através do sistema RSA, devemos seguir os passos descritos abaixo.

1) **Escolhemos dois números primos distintos m e n, e calculamos $k = m \cdot n$.** Quanto maior os números m e n, mais seguro será o código, assim garantimos que a chave não seja quebrada facilmente. No entanto, para facilitar os cálculos e também o entendimento, adotamos aqui, para m e n, valores pequenos, por exemplo, $m = 2$ e $n = 5$. Logo, $k = 2 \cdot 5 = 10$.

2) **Agora, escolhemos um número p que não tenha fatores comuns e que obedeça a desigualdade**

$$p < (m-1) \cdot (n-1)\,.$$

Assim, vamos ter, no nosso exemplo:

$$p < (2-1).(5-1) \Rightarrow p < 1.4 \Rightarrow p < 4 \Rightarrow p \in \{2,3\}.$$

Adotamos o valor $p = 3$.

3) **Encontramos agora, um número q, com $q \neq p$, tal que o valor da expressão $p \cdot q - 1$ seja um múltiplo de $(m-1) \cdot (n-1)$.** No nosso exemplo, múltiplo de 4. Escolhemos $q = 7$, pois $p \cdot q - 1 = 3.7 - 1 = 21 - 1 = 20$, e 20 é múltiplo de 4. Com esses dados, podemos estabelecer as chaves para cifrar e decifrar mensagens:

Tabela 4 – Chaves de codificação e decodificação

Chave pública	Chave privada
(k,p)	(k,q)
(10,3)	(10,7)

Fonte: Autor

Como $k = 10$, adotamos apenas nove letras do alfabeto escolhidas arbitrariamente e pré-codificadas, substituídas pelos números, conforme tabela 5 abaixo.

Tabela 5 – Letras arbitrárias pré-codificadas

P	M	A	F	E	O	R	T	C
1	2	3	4	5	6	7	8	9

Fonte: Autor

Os números p e q serão usados para construir as funções bijetoras $f(x)$ e $h(x)$:

$$\begin{array}{ccc} f:\{1,2,3,4,5,6,7,8,9\} & \longrightarrow & \{1,2,3,4,5,6,7,8,9\} \\ x & \longrightarrow & f(x) \end{array}$$

e

$$\begin{array}{ccc} h:\{1,2,3,4,5,6,7,8,9\} & \longrightarrow & \{1,2,3,4,5,6,7,8,9\} \\ x & \longrightarrow & h(x) \end{array},$$

tais que $f(h(x)) = h(f(x)) = i(x)$, em que

$$\begin{array}{ccc} i:\{1,2,3,4,5,6,7,8,9\} & \longrightarrow & \{1,2,3,4,5,6,7,8,9\} \\ x & \longrightarrow & i(x) = x \end{array}$$

é a função identidade.

A função $f(x)$ será definida como o resto da divisão de x^p por k, com $k \neq 0$. Logo, temos, aplicando os valores particulares do nosso exemplo, $f(4) = 4$, pois $\frac{4^3}{10} = \frac{64}{10}$ e $64 = 6.10 + 4$, ou seja, 60 deixa resto 4 na divisão por 10, portanto, $f(4) = 4$. Assim, podemos construir a tabela 6 abaixo.

Tabela 6 – Aplicação da função $f(x)$ para codificar a mensagem

x	1	2	3	4	5	6	7	8	9
x^3	1	8	27	64	125	216	343	512	729
$f(x)$	1	8	7	4	5	6	3	2	9

Fonte: Autor

Como exemplo, vamos codificar a palavra **PROFMAT**.

Pela pré-codificação dada na tabela 5, segue:

P	R	O	F	M	A	T	
1	7	6	4	2	3	8	$\rightarrow$ tabela 5 - pré-codificação

Pela codificação dada pela tabela 6, aplicando a função $f(x)$, teremos:

1	7	6	4	2	3	8	$\rightarrow$	tabela 5 - pré-codificação
1	3	6	4	8	7	2	$\rightarrow$	tabela 6 - aplicando $f(x)$
P	A	O	F	T	R	M	$\rightarrow$	convertendo $f(x)$ para a tabela 5

Portanto, a palavra **PROFMAT**, codificada usando o sistema RSA é **PAOFTRM**.

Para decifrar a mensagem, aplicamos a função inversa $h(x)$, definida como sendo o resto da divisão de x^q por k, com $k \neq 0$. Logo, temos, em particular, $h(2) = 8$, já que $\frac{2^7}{10} = \frac{128}{10}$ e $128 = 12.10 + 8$, isto é, 128 deixa resto 8 na divisão por 10. Assim, podemos construir a tabela 7 a seguir:

Tabela 7 – Aplicação da função inversa $h(x)$ para decodificar a mensagem

x	1	2	3	4	5	6	7	8	9
x^7	1	128	2187	16384	78125	279936	823543	2097152	4782969
$h(x)$	1	8	7	4	5	6	3	2	9

Fonte: Autor

Agora vamos decifrar a palavra **PAOFTRM**.

Pela pré-codificação dada pela tabela 5, segue:

P	A	O	F	T	R	M	
1	3	6	4	8	7	2	$\rightarrow$ tabela 5 - pré-codificação

Pela decodificação dada pela tabela 7, aplicando a função $h(x)$, teremos:

1	3	6	4	8	7	2	$\rightarrow$	tabela 5 - pré-codificação
1	7	6	4	2	3	8	$\rightarrow$	tabela 7 - aplicanco $h(x)$
P	R	O	F	M	A	T	$\rightarrow$	convertendo $h(x)$ para a tabela 5

Portanto, a palavra **PAOFTRM**, decifrada usando o sistema RSA, é **PROFMAT**.

O sistema RSA[5] é o método de criptografia mais utilizado no mundo.

2.7 O manuscrito Voynich

Ao longo da história, a batalha travada entre criptógrafos e criptoanalistas parece não ter fim. Durante séculos, os criptógrafos introduziam suas cifras, aparentemente indecifráveis, e os criptoanalistas, com habilidade, inteligência e dedicação, conseguiam de uma forma ou de outra decifrá-las. Mesmo as cifras mais poderosas, como a cifra de Vigenère e o sistema Enigma de cifragem, não foram capazes de permanecer invulneráveis ao longo dos séculos. Neste cenário, os criptoanalistas mantêm certa vantagem. No entanto, existem sistemas de criptografia que permanecem até hoje, praticamente indecifráveis. O manuscrito de Voynich é um exemplo de que a batalha entre os codificadores e os decifradores de códigos recuperou o equilíbrio, pois até hoje, criptoanalistas espalhados pelo mundo, convergem seus esforços para decifrá-lo.

> Pouco se sabe sobre o manuscrito e sua história. Apenas que está escrito em um alfabeto inventado, jamais visto em outro documento, e que foi adquirido em 1912, perto de Roma, na Itália, por um livreiro polonês chamado Wilfrid Voynich, que se casou com a filha de George Boole, famoso matemático britânico. O manuscrito é ricamente ilustrado com imagens de plantas e corpos celestes, o que sugere que se trate de um texto sobre ervas e astrologia. Mas seu conteúdo continua um enigma (ZOLNERKEVIC, 2013, p. 60).

A figura 12 mostra uma das várias ilustrações de plantas do manuscrito Voynich. Essas ilustrações, são na maioria desconhecidas, porém essa assemelha-se a um girassol.

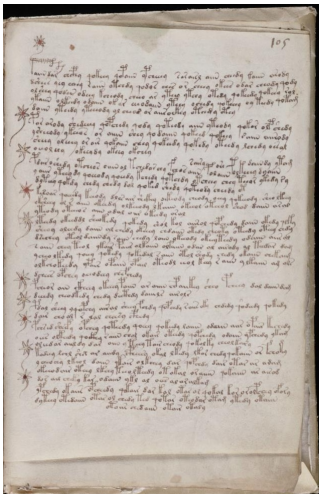
[5] A descrição completa do funcionamento do RSA encontra-se no livro Criptografia de Severino Collier Coutinho. Rio de Janeiro, IMPA, 2015. Distribuição: IMPA/OBMEP.

Figura 12 – Ilustração de plantas no manuscrito Voynich

Fonte: Zolnerkevic (2013)

Segundo Portilho (2018), o intrigante no manuscrito Voynich é a unicidade de seu alfabeto. Ele foi escrito sem pontuação e constituído por aproximadamente 170 mil caracteres que compõe em torno de 35 mil palavras indecifráveis. Outro detalhe é a sua total ausência de erros ortográficos (não existem rasuras). Além do alfabeto enigmático, o Voynich também apresenta diagramas que parecem se referir a estrelas e signos. Possui figuras femininas, quase sempre imersas até os joelhos em estranhos vasos contendo um fluido escuro. Também apresenta uma grande variedade de ilustrações de plantas, em sua maioria desconhecidas. Entre essas diversas ilustrações de plantas, uma é supostamente parecida com um girassol. No entanto, pelos cálculos feitos com testes de carbono 14, acredita-se que o livro tenha sido escrito há cerca de 600 anos, portanto, anterior à origem do cultivo de girassol na Europa, tornando o Voynich mais misterioso ainda. O livro é dividido em seções: biologia, botânica, astronomia e farmacologia.

Figura 13 – Um exemplo do texto do manuscrito Voynich



Fonte: Portilho (2018)

Após a morte de Wilfrid Michael Voynich (1865 – 1930), o manuscrito foi parar na Universidade Yale, EUA, e passou a ser o item MS 408 na Beinecke Rare Book and Manuscript Library da Universidade, onde é estudado até hoje.

Portanto, observou-se que a criptografia esteve presente em grandes acontecimentos de nossa história e, atualmente, com a evolução dos meios de comunicação, ela está sendo amplamente utilizada. Para dar continuidade ao objetivo desta dissertação, em que se pretende apresentar a criptografia como uma ferramenta para contextualizar o conteúdo de funções afins, apresenta-se no próximo capítulo, um estudo sobre funções.

3 FUNÇÕES

Em seu livro *Tópicos de História da Matemática*, Roque e Carvalho (2012) descrevem as primeiras noções de função. O conceito de função surgiu após as técnicas de derivação introduzidas por Gottfried Wilhelm Leibniz (1646 – 1716) e Isaac Newton (1643 – 1727). O conceito de função nos sugere a ideia de uma correspondência. Deste ponto de vista, as tabelas babilônicas e egípcias já conjecturavam, de certa forma, o discernimento de função, uma vez que elas tratavam de registros de correspondências, por exemplo, entre um número e o resultado das operações que envolvem este número.

Segundo Roque e Carvalho (2012), o destaque em relação à idealização de correspondência fez com que alguns historiadores da Matemática percebessem um precedente no entendimento de função nas tabelas babilônicas e egípcias. No entanto os egípcios e os babilônios não tinham nessa época a noção de função dada pela correspondência de valores.

Ainda, segundo Roque e Carvalho (2012), outra abordagem no conceito de função que temos atualmente é a variação. A ideia de variável só foi introduzida formalmente no século XIX, porém, essa noção já estava presente em estudos realizados no período da revolução científica dos séculos XVI e XVII. René Descartes (1596 – 1650) trabalhava com equações indeterminadas, nas quais, tomando-se infinitos valores para a variável x, é possível encontrar infinitos valores para y.

> No estudo de curvas descritas por equações indeterminadas, está presente a ideia de que uma equação em x e y é um modo de representar uma dependência entre duas quantidades variáveis, de modo que se possam calcular os valores de uma delas por meio dos valores da outra (ROQUE; CARVALHO, 2012, p. 265).

Assim, a relação entre as quantidades indeterminadas estudadas nas curvas por Descartes era do tipo funcional, pois associava uma quantidade à outra por meio de uma equação. Implicitamente, esse tipo de relação entre variáveis era dada por expressões analíticas de curvas algébricas ou por meio de séries infinitas.

Segundo Roque e Carvalho (2012), a ampliação desse conceito foi dada por Leibniz, quando se expandiu o universo das curvas, para incluir os transcendentes, que podiam ser representados por séries infinitas construindo a base da definição de função do século XVIII. Dessa maneira, a função foi definida como uma expressão analítica composta de um modo qualquer de quantidades constantes e variáveis. Mais tarde, no início do século XX, com o desenvolvimento da noção de conjunto, levou a redefinir as noções centrais da Matemática. A partir daí, a teoria dos conjuntos passou a ser o ajustamento mais adequado na obtenção de uma nova concordância sobre os fundamentos da análise e de toda a Matemática, mudando assim a concepção sobre número e função.

Em 1718, Jean Bernoulli (1667 – 1748) apresentou à Academia de Ciências de Paris um novo discernimento de função. “Chamamos função de uma grandeza variável uma quantidade composta, de um modo qualquer, desta grandeza variável e de constantes” (Opera omnia, p. 241 apud Roque; Carvalho, 2012, p. 301).

Leonhard Paul Euler (1707 – 1783) foi o precursor no tratamento do cálculo como uma teoria das funções. Em seu livro intitulado *Introdução à análise dos infinitos*, Euler, logo no início, apresenta uma definição de função: “Uma função de uma quantidade variável é uma expressão analítica composta de um modo qualquer desta quantidade e de números, ou de quantidades constantes.” (Opera omnia, p. 17 apud Roque; Carvalho, 2012, p. 302). Para Euler, função só eram as contínuas e não era somente a expressão analítica, mas “a curva traçada a mão livre” e ainda sem “cantos”.

Segundo Roque e Carvalho (2012), Jean le Rond d’Alembert (1717 – 1783), em seus estudos das vibrações infinitamente pequenas de uma corda presa por suas extremidades, problema da corda vibrante[6], dá uma solução que pode ser representada pela soma de duas funções arbitrárias nas variáveis x e t: $\theta(x+at)$ e $\theta(x-at)$, em que θ é uma função arbitrária sujeita a certas condições dependendo do comprimento da corda e das condições iniciais. Mais tarde, Daniel Bernoulli (1700 – 1782) dá outra solução para o mesmo problema das cordas vibrantes em forma de série de funções trigonométricas.

Segundo Correia (1999), Jean Baptiste Joseph Fourier (1768 – 1830), matemático francês que iniciou a investigação sobre a decomposição de funções periódicas em séries trigonométricas convergentes, chamadas séries de Fourier, descobre que uma função pode ter diferentes expressões analíticas e também que pode ser descontínua.

Conforme Sierpinska (1992), foi Peter Gustav Lejeune Dirichlet (1805 – 1859) matemático alemão, a quem se atribui a moderna definição de função. Dirichlet mostrou que o conceito de função vai além da continuidade, é mais geral. Em 1837, ele propôs a seguinte definição geral de função:

> Se uma variável y está tão relacionada a uma variável x que sempre que um valor numeral é atribuído a x existe uma regra segundo a qual um valor único de y é determinado, então y é dito ser uma função da variável independente x (SIERPINSKA, 1992, p. 46, tradução nossa).

De acordo com Silva (2015), influenciados pelos trabalhos de Dirichlet, Julius Wilhelm Richard Dedekind (1831 – 1916) e Georg Friedrich Bernhard Riemann apresentaram o conceito de função sob a seguinte caracterização:

[6] O problema da corda vibrante, trata-se do estudo das vibrações infinitamente pequenas de uma corda presa por suas extremidades: Uma corda elástica com extremidades fixas 0 e l é deformada até uma posição inicial, em seguida liberada; a corda começará a vibrar e o problema é o de determinar a função que descreve a forma da corda em um instante t.

> Uma aplicação φ de um sistema S é uma lei, que associa a cada elemento s de S uma certa coisa, que é chamada imagem de s e que escrevemos $\varphi(s)$, onde o domínio e contradomínio podem ser qualquer conjunto, não somente de número, mas de matrizes, vetores, e mesmo de funções (BOYER; MERZBACH, 2012, apud SILVA, 2015, p. 18).

Portanto, o conceito de função foi sendo definido gradativamente. O que hoje conhecemos como função é resultado de trabalhos e experiências que se somaram ao longo dos séculos, contribuindo, de certa maneira, com o desenvolvimento da Matemática e, consequentemente, com o progresso de nossa ciência.

3.1 O estudo das funções segundo PCN e BNCC

Segundo os Parâmetros Curriculares Nacionais (PCN), BRASIL (1998, p. 115), "o estudo da Álgebra desenvolve no educando a capacidade de abstração e generalização, além de viabilizar condições necessárias na resolução de problemas." Ao introduzir variáveis para representar relações funcionais em situações-problema, possibilita-se ao aluno expandir seus conhecimentos, uma vez que ele percebe novas funções para o uso das letras ao identificá-las como números de um conjunto numérico, úteis para representar generalizações.

> As situações-problema sobre variações de grandezas fornecem excelentes contextos para desenvolver a noção de função. Os alunos podem, por exemplo, estabelecer como varia o perímetro (ou a área) de um quadrado, em função da medida de seu lado; determinar a expressão algébrica que representa a variação, assim como esboçar o gráfico cartesiano que representa essa variação (BRASIL, 1998, p. 118).

Diversas aplicações envolvendo funções abordadas no quarto ciclo (7^a e 8^a), especificamente a 8^a série, hoje correspondentes ao 9^o ano do Ensino Fundamental, são enfatizadas nos PCNs, BRASIL (1998). No texto, além das situações propostas para verificar a variação do perímetro (ou área) de polígonos, em função da medida de seus lados, também se destaca a importância dos gráficos para o desenvolvimento de conceitos e procedimentos algébricos e para mostrar a variedade de relações possíveis entre duas variáveis. Também são sugeridas situações-problema para serem aplicadas aos alunos, de modo que desenvolvam sequências de operações para obter os preços no varejo e no atacado e depois determinem a expressão algébrica que permite calcular o preço no atacado em função do preço de custo.

A Base Nacional Comum Curricular (BNCC) do Ensino Fundamental, é uma proposta apresentada em 2015 e, posteriormente, em abril de 2016, foi lançada a público sua 2^a versão revista. Ela tem por finalidade, apresentar direitos de aprendizagem na forma de objetivos, que direcionam o currículo da Educação Básica. No que se refere à

área Matemática, a BNCC, nas séries finais do Ensino Fundamental, relacionada ao eixo álgebra e funções, faz a seguinte menção:

> O trabalho com a álgebra e funções, nos anos finais do Ensino Fundamental, retoma e amplia o que é estudado nos anos iniciais. Dessa forma, nos anos finais, as ideias de regularidade, de generalização e de equivalência se constituem também em alicerces para o desenvolvimento de outras dimensões da álgebra, como a resolução de problemas de estrutura algébrica e a noção de função. É nesse momento que as noções de variável e de incógnita, em que letras são utilizadas para representar números desconhecidos, ganham corpo na representação de sentenças matemáticas, como expressões algébricas e equações (BRASIL, 2016, p. 432).

As habilidades mencionadas na BNCC, BRASIL (2016), no que se refere às funções, estão relacionadas em compreender as funções como relações de dependência unívoca entre duas variáveis e suas representações numéricas, algébricas e gráficas e também utilizar esse conceito para analisar situações que envolvem relações funcionais entre duas variáveis.

Assim, pode-se notar que os PCNs, hoje atualizado pela BNCC, nos anos finais do Ensino Fundamental, fazem referências à importância do estudo das funções, uma vez que contribui com o desenvolvimento do raciocínio lógico e estabelece relações quantitativas entre grandezas e variáveis. As funções estão presentes no cotidiano do educando, portanto, sua aprendizagem é essencial para o desenvolvimento dos saberes matemáticos, pois sua aplicabilidade pode ser inserida nas situações vivenciadas por ele.

3.2 Conceito de função

As funções estão presentes em nosso cotidiano, seja em casa, no trabalho ou mesmo no lazer. Por esse motivo, seu conceito é indispensável na formação de nosso aprendizado. Antes de abordar o conceito de função, faremos um breve comentário sobre produto cartesiano e relações binárias.

3.3.1 Produto cartesiano e relação binária

Segundo Iezzi e Murakami (1977), dados dois conjuntos A e B não vazios, denomina-se *produto cartesiano* de A por B o conjunto $A \times B$ cujos elementos são todos pares ordenados (x, y) tal que $x \in A$ e $y \in B$.

Escrevemos $A \times B = \{(x, y) \mid x \in A \text{ e } y \in B\}$ para denotar o *produto cartesiano* de A por B.

Uma *relação binária* entre dois conjuntos A e B é qualquer subconjunto R do *produto cartesiano* entre o conjunto A e o conjunto B. Ou seja, R é *relação binária* de A em $B \Leftrightarrow R \subset A \times B$.

Vejamos alguns exemplos.

Exemplo 3.1. *Sejam os conjuntos* $A = \{1,2,3,4\}$ *e* $B = \{1,4,16\}$ *e consideremos as relações de* A *em* B*, definidas por* R_1 *e* R_2*, tais que*

$$R_1 = \{(x,y) \mid x = \sqrt{y}\} \text{ e } R_2 = \{(x,y) \mid x = \frac{y}{3}\}.$$

Podemos dizer que R_1 *e* R_2 *representam relações binárias de* A *em* B*?*

Solução. *Primeiramente, vamos determinar o produto cartesiano de* A *por* B*, isto é,* $A \times B$*. Pela definição,* $A \times B = \{(a,b) \mid a \in A \text{ e } b \in B\}$*, assim,*

$$A \times B = \{(1,1),(1,4),(1,16),(2,1),(2,4),(2,16),(3,1),(3,4),(3,16),(4,1),(4,4),(4,16)\}.$$

Portanto, o subconjunto $R_1 = \{(1,1),(2,4),(4,16)\} \subset A \times B$*, obtido a partir da relação*

$$R_1 = \{(x,y) \mid x = \sqrt{y}\}$$

é uma relação binária de A *em* B*, já a relação* R_2 *não é uma relação binária de* A *em* B*, pois não existe nenhum elemento de* A *que seja a terça parte de um elemento de* B*.*

3.3.2 O conceito de função por meio de diagramas

É comum, professores da Educação Básica, utilizarem os diagramas para ilustrar o conceito de funções.

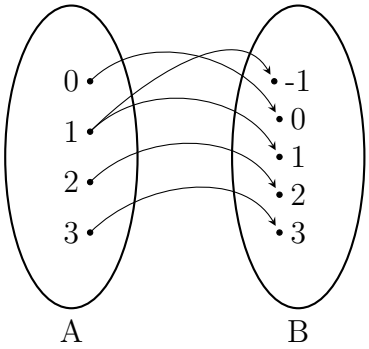
Em seu livro *Fundamentos de Matemática Elementar* vol. 1, Iezzi e Murakami (1977) tratam de maneira simples e clara sobre o conceito apresentado de função.

Consideremos os conjuntos $A = \{0,1,2,3\}$ e $B = \{-1,0,1,2,3\}$ e tomemos as seguintes *relações binárias* de A em B:

- $R_1 = \{(x,y) \in A \times B \mid y^2 = x^2\}$;
- $R_2 = \{(x,y) \in A \times B \mid y = x+1\}$;
- $R_3 = \{(x,y) \in A \times B \mid y = (x-1)^2 - 1\}$.

Na relação $R_1 = \{(0,0),(1,-1),(1,1),(2,2),(3,3)\}$, observamos que nem todo elemento $x \in A$ corresponde um único elemento $y \in B$ tal que $(x,y) \in R_1$, pois existe o elemento $1 \in A$ correspondente a dois elementos $y \in B$, a saber, $(1,-1) \in R_1$ e $(1,1) \in R_1$, conforme diagrama a seguir:

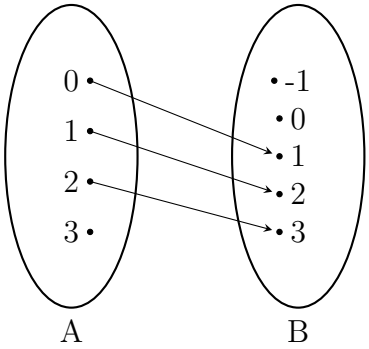
Figura 14 – Diagrama da relação R_1



Fonte: Autor

Já na relação $R_2 = \{(0,1),(1,2),(2,3)\}$, o elemento $3 \in A$ não corresponde a nenhum elemento $y \in B$, ou seja, não existe $y \in B$ tal que $(3,y) \in R_2$, vejamos o diagrama abaixo:

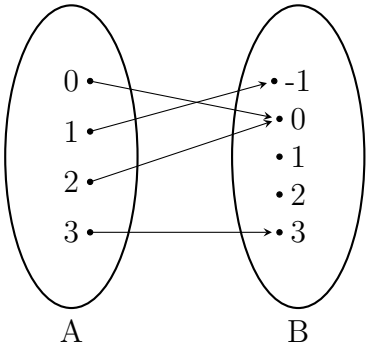
Figura 15 – Diagrama da relação R_2



Fonte: Autor

Agora observemos o diagrama $R_3 = \{(0,0),(1,-1),(2,0),(3,3)\}$. Nessa relação, verificamos que para todo elemento $x \in A$, sem exceção, existe um único elemento $y \in B$ tal que $(x,y) \in R_3$, segue diagrama a seguir:

Figura 16 – Diagrama da relação R_3



Fonte: Autor

A relação R_3, em particular, que possui a característica de que todo elemento $x \in A$ corresponde a um, e somente um elemento $y \in B$ tal que $(x, y) \in R_3$, recebe o nome de função definida em A com imagem em B ou uma aplicação de A em B.

Como dito, a formalização do conceito de função, foi sendo construída gradativamente ao longo dos séculos. Atualmente, uma função pode ser assim definida:

> Dados dois conjuntos A, $B \subset \mathbb{R}$, não vazios, uma relação f de A em B recebe o nome de aplicação de A em B ou função definida em A com imagens em B se, e somente se, para todo $x \in A$ existe um só $y \in B$ tal que $(x, y) \in f$ (IEZZI; MURAKAMI, 1977, p. 74-A).

Podemos reescrever a definição acima da seguinte forma:

$$f \text{ é aplicação de } A \text{ em } B \Leftrightarrow \forall\ x \in A,\ \exists!\ y \in B \text{ tal que } (x, y) \in f.$$

O conjunto A é chamado de domínio e o conjunto B de contra-domínio da função f.

Então, podemos dizer que uma função f de A em B é uma regra (ou conjunto de instruções) que nos diz como associar a cada elemento x em A um único elemento y em B. A natureza da regra que diz como obter tal elemento y quando é dado x é inteiramente arbitrária, porém é sujeita a apenas duas condições:

a) *Não pode haver exceções,* esta condição é para garantir que a função f tenha o conjunto A como domínio.

b) *Não pode haver ambiguidade,* garante a unicidade de y para cada x.

Existem vários exemplos de funções, mas restrigiremos as funções afins.

3.3 Função afim

Em seu livro *Números e Funções Reais*, Lima (2014) diz que uma função $f : \mathbb{R} \to \mathbb{R}$ chama-se afim quando existem constantes a, $b \in \mathbb{R}$ tais que $f(x) = ax + b$ para todo $x \in \mathbb{R}$. Também são funções afins:

- A *função identidade*: $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x$, para todo $x \in \mathbb{R}$;
- As *translações*: $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x + b$, para todo $x \in \mathbb{R}$;
- As *funções lineares*: $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = ax$, para todo $x \in \mathbb{R}$;
- E as *funções constantes*: $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = b$, para todo $x \in \mathbb{R}$.

Nem sempre os coeficientes a e b de uma determinada função $f:\mathbb{R}\to\mathbb{R}$ são explícitos, mesmo assim, é possível saber se essa função é afim. Neste caso, o coeficiente b pode ser obtido como o valor que a função dada assume quando $x=0$. Com efeito, sabemos que a função afim é definida pela relação $f(x)=ax+b$, com $a,b\in\mathbb{R}$. Quando $x=0$, obtemos que $f(0)=a.0+b=b$. O número b é chamado de valor inicial da função f. Agora, se conhecermos dois valores $f(x_1)$ e $f(x_2)$ que a função f assume em dois pontos distintos quaisquer x_1 e x_2 do domínio, podemos determinar o coeficiente a. De fato, para $f(x_1)=ax_1+b$ e $f(x_2)=ax_2+b$, temos

$$f(x_2)-f(x_1)=ax_2+b-(ax_1+b)=a(x_2-x_1),$$

portanto

$$a=\frac{f(x_2)-f(x_1)}{x_2-x_1}.$$

Em particular, dados $x_1=p,\ x_2=p+q\ \in\ \mathbb{R}$, com $p,q\ \in\ \mathbb{R},\ q\neq 0$, o número $a=\frac{f(p+q)-f(p)}{q}$ chama-se a taxa de crescimento (ou taxa de variação) da função f no intervalo de extremos p, $p+q$. É essa taxa de crescimento (dada pelo coeficiente a) que indica se a função afim é crescente ($a>0$), decrescente ($a<0$) ou constante ($a=0$).

Em geral, temos que dados $x_1,x_2,y_1,y_2\in\mathbb{R}$, com $x_1\neq x_2$, existe uma única função afim $f:\mathbb{R}\longrightarrow\mathbb{R}$ tal que $f(x_1)=y_1$ e $f(x_2)=y_2$.

3.4.1 Gráfico da função afim

Segundo Lima (2014), o gráfico de uma função afim $f:x\mapsto ax+b$ é uma reta.

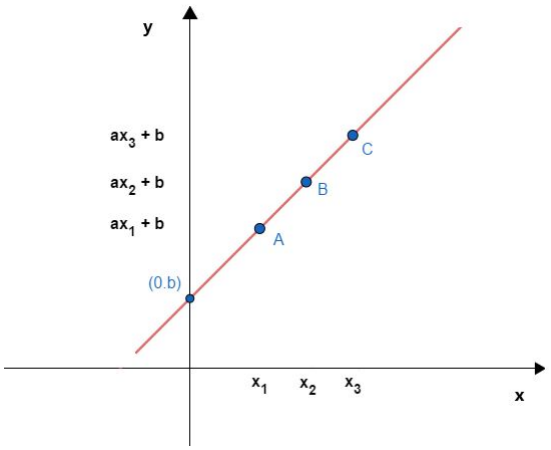
Para verificarmos essa afirmação, precisamos utilizar a fórmula da distância entre dois pontos no plano: Dados pontos $A=(x_1,y_1)$ e $B=(x_2,y_2)$ no plano, a distância entre A e B, a qual denotamos por $d(A,B)$, é

$$d(A,B)=\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}.$$

Munidos dessa fórmula, destacaremos três pontos quaisquer, distintos dois a dois, do gráfico e provaremos que eles são colineares.

Sejam A, B e C três pontos quaisquer do gráfico tais que $A=(x_1,ax_1+b)$, $B=(x_2,ax_2+b)$ e $C=(x_3,ax_3+b)$. Para provarmos que A, B e C pertencem à mesma reta, é necessário e suficiente que o maior número entre $d(A,B)$, $d(B,C)$ e $d(A,C)$ seja igual à soma dos outros dois. Sem perda de generalidade, suponhamos que as abscissas x_1, x_2 e x_3 são tais que $x_1<x_2<x_3$ e aplicaremos a fórmula da distância entre dois pontos para provar que $d(A,C)=d(A,B)+d(B,C)$.

Figura 17 – Gráfico de uma função afim



Fonte: Autor

Temos que

$$\begin{aligned} d(A,B) = \sqrt{(x_2-x_1)^2+[ax_2+b-(ax_1+b)]^2} &= \sqrt{(x_2-x_1)^2+(ax_2-ax_1)^2} \\ &= \sqrt{(x_2-x_1)^2+a^2(x_2-x_1)^2} \\ &= \sqrt{(x_2-x_1)^2(1+a^2)} \\ &= (x_2-x_1)\sqrt{1+a^2}. \end{aligned}$$

Analogamente,

$$d(B,C) = (x_3-x_2)\sqrt{1+a^2} \text{ e } \ d(A,C) = (x_3-x_1)\sqrt{1+a^2}.$$

Daí,

$$\begin{aligned} d(A,B)+d(B,C) = (x_2-x_1)\sqrt{1+a^2}+(x_3-x_2)\sqrt{1+a^2} &= \sqrt{1+a^2}(x_2-x_1+x_3-x_2) \\ &= \sqrt{1+a^2}(x_3-x_1) \\ &= d(A,C). \end{aligned}$$

Portanto,

$$d(A,B)+d(B,C) = d(A,C).$$

Exemplo 3.2. *(UFPE–1979) A altura h de um homem varia com o tamanho f do seu fêmur, de acordo com a seguinte fórmula: $h(f) = 69,089+2,238f$ (medidas expressas em cm). Se a idade ultrapassar 30 anos, subtrai-se $0,06cm$ por cada ano após os 30 anos. Qual a altura estimada de um homem de 40 anos cujo fêmur mede $40cm$?*

Solução. *Foi dado no enunciado que $h(f) = 69,089+2,238f$, assim, substituindo $f = 40$, temos que*

$$h(40) = 69,089+2,238\times 40 \Rightarrow h(40) = 69,089+89,52 \Rightarrow h(40) = 158,609cm.$$

Como, após os 30 anos, deve-se subtrair 0,06cm a cada ano ultrapassado, temos:

$$40-30=10 \Rightarrow 10\times 0,06cm=0,6cm \Rightarrow 158,609cm-0,6cm=158,009cm.$$

Portanto, a altura estimada dessa pessoa é $1,58m$.

3.4 Função injetora

Segundo Iezzi e Murakami (1977), uma função f é uma *injeção* de A e B se, e somente se, quaisquer que sejam x_1, $x_2 \in A$, se $x_1 \neq x_2$ então $f(x_1) \neq f(x_2)$.

Ou seja, uma função f de A em B indicada por $f : A \to B$ é *injetiva* quando

$$x_1 \neq x_2 \text{ em } A \Rightarrow f(x_1) \neq f(x_2).$$

Esta condição pode também ser expressa da seguinte forma:

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Exemplo 3.3. *A função de* $A=\mathbb{R}^*$ *em* $B=\mathbb{R}$ *definida por* $f(x)=\frac{1}{x}$ *é injetora, pois, quaisque que sejam* x_1 *e* x_2 *de* $\mathbb{R}^*$*, se* $x_1 \neq x_2$*, então* $\frac{1}{x_1} \neq \frac{1}{x_2}$.

3.5 Função sobrejetora

Para Iezzi e Murakami (1977), uma função f é uma *sobrejeção* de A em B se, e somente se, para todo $y \in B$ existe um elemento $x \in A$ tal que $f(x) = y$.

Ou seja, $f : A \to B$ é *sobrejetiva* $\Leftrightarrow \forall\ y \in B,\ \exists\ x \in A$ tal que $f(x) = y$.

Portanto, percebemos que $f : A \to B$ é *sobrejetiva* se, e somente se, $Im(f) = B$, em que $Im(f) = \{y \in B \mid \exists\ x \in A \text{ com } f(x) = y\}$ é o conjunto imagem da função f.

Exemplo 3.4. *A função* f *de* $A=\{-1,0,1,2\}$ *em* $B=\{0,1,4\}$ *definida por* $f(x)=x^2$ *é sobrejetora, pois, para todo elemento* $y \in B$*, existe o elemento* $x \in A$ *tal que* $y=x^2$.

3.6 Função bijetora

Ainda segundo Iezzi e Murakami (1977), uma função f de A em B é uma *bijeção* se, e somente se, para qualquer elemento $y \in B$ existe um único elemento $x \in A$ tal que $f(x) = y$. Assim, temos:

$$f : A \to B \text{ é } \textit{bijetiva} \Leftrightarrow \forall y \in B,\ \exists!\ x \in A \text{ tal que } f(x) = y.$$

Então, a definiçao nos permite concluir que uma função f de A em B é uma *bijeção* se, e somente se, f é uma *injeção* e uma *sobrejeção*.

Exemplo 3.5. *A função f de $A=\mathbb{R}$ em $B=\mathbb{R}$ definida por $f(x)=3x+2$ é bijetora, pois:*

i) Qualquer que seja $y\in\mathbb{R}$, existe $x\in\mathbb{R}$ tal que $y=3x+2$. Para tal, basta tomarmos $y=3x+2\Rightarrow 3x=y-2\Rightarrow x=\frac{y-2}{3}$. Logo, f é sobrejetora;

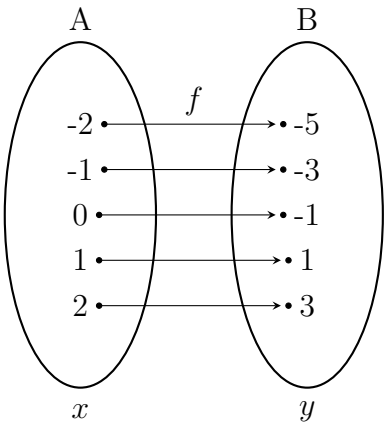
ii) Quaisquer que sejam x_1 e x_2 de $\mathbb{R}$, se $x_1\neq x_2$, então $3x_1+2\neq 3x_2+2$, isto é, f é injetora.

Portanto, f é injetora e sobrejetora. Logo, f é uma bijeção de A em B.

3.7 Função inversa

Dados os conjuntos $A=\{-2,-1,0,1,2\}$ e $B=\{-5,-3,-1,1,3\}$, consideremos a função f de A em B definida por $y=2x-1$.

Figura 18 – Diagrama da função f de A em B definida por $y=2x-1$



Fonte: Autor

A função f de A em B é uma *bijeção* formada pelos pares ordenados:
$f=\{(-2,-5),(-1,-3),(0,-1),(1,1),(2,3)\}$, em que o domínio da função f é igual ao conjunto A indicado por $D(f)=A$ e a imagem da função f é igual ao conjunto B indicada por $Im(f)=B$.

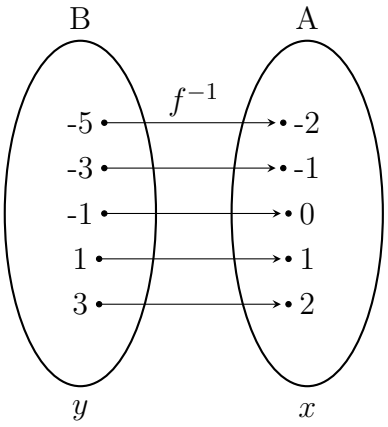
Agora consideremos a relação

$$f^{-1}=\{(y,x)\mid (x,y)\in f\}=\{(-5,-2),(-3,-1),(-1,0),(1,1),(3,2)\}.$$

Esta relação é uma função, pois f é uma *bijeção* de A em B, isto é, para todo $y\in B$ existe um único $x\in A$ tal que $(y,x)\in f^{-1}$, e esta é a função inversa de f. O domínio da função f^{-1} é igual ao conjunto B indicado por $D(f^{-1})=B$ e a imagem da função f^{-1} é igual ao conjunto A indicada por $Im(f^{-1})=A$

Observamos que a regra que associa a cada $y\in B$ a um único $x\in A$ é dada por $f^{-1}(y)=\dfrac{y+1}{2}=x$.

Figura 19 – Diagrama da função f^{-1} de B em A definida por $x = \frac{y+1}{2}$



Fonte: Autor

Segundo Lima (2014, p. 162), "a função $g : Y \to X$ é a inversa da função $f : X \to Y$ quando se tem $g(f(x)) = x$ e $f(g(y)) = y$ para quaisquer $x \in X$ e $y \in Y$. Evidentemente, g é a inversa de f se, e somente se, f é a inversa de g."

Ainda para Iezzi e Murakami (1977), a função inversa, os pares ordenados que formam f^{-1} podem ser obtidos dos pares ordenados de f, permutando-se os elementos de cada par, isto é:

$$(x, y) \in f \Leftrightarrow (y, x) \in f^{-1}.$$

Agora, se considerarmos a função inversa de f^{-1}, teremos:

$$(y, \ \ x) \in f^{-1} \Leftrightarrow (x, \ \ y) \in \left(f^{-1}\right)^{-1}$$

Isto é, a inversa de f^{-1} é a própria função f:

$$(f^{-1})^{-1} = f.$$

Podemos assim afirmar que f e f^{-1} *são inversas entre si*, ou seja, uma é inversa da outra.

Como visto na figura 19, o domínio da função f^{-1} é B, que é a imagem da função f, a imagem da função f^{-1} é A, que é o domínio da função f.

Teorema 1. *Seja $f : A \to B$. A relação f^{-1} é uma função de B em A se, e somente se, f é bijetora.*

Demonstração. *Suponhamos que f^{-1} é uma função de B em A. Queremos mostrar que f é bijetora. De fato, pela definição de função, dado $y \in B$ existe um único $x \in A$ tal que $f^{-1}(y) = x$, isto é, $(y, \ \ x) \in f^{-1}$, ou ainda, $(x, \ \ y) \in f$. Assim, f é sobrejetora. Agora,*

dados $x_1 \in A$ e $x_2 \in A$, com $x_1 \neq x_2$, se $f(x_1) = f(x_2) = y$, obteremos que $f^{-1}(y) = x_1$ e $f^{-1}(y) = x_2$, o que contradiz f^{-1} ser uma função, pois y só pode ter uma imagem em f^{-1}. Assim, $f(x_1) \neq f(x_2)$ e, portanto, f é injetora. Logo, f é bijetora.

Agora, suponhamos que f é bijetora, queremos mostrar que f^{-1} é uma função de B em A. Como f é sobrejetora, para todo $y \in B$ existe $x \in A$ tal que $(x,y) \in f$, portanto, $(y,x) \in f^{-1}$, isso mostra que não há exceções. Seja $y \in B$ tal que existem x_1 e x_2 em A com $(y,x_1) \in f^{-1}$ e $(y,x_2) \in f^{-1}$, então $(x_1,y) \in f$ e $(x_2,y) \in f$. Como f é injetora, $x_1 = x_2$, ou seja, não há ambiguidade. Logo, f^{-1} está bem definida, isto é, é uma função. Concluímos assim o resultado.

Exemplo 3.6. *Determinar a função inversa de $f : \mathbb{R} - \{\frac{1}{3}\} \to \mathbb{R} - \{\frac{5}{3}\}$, definida por $f(x) = \frac{5x+2}{3x-1}$.*

Solução. *Como $f(x) = y$, escrevemos $y = \frac{5x+2}{3x-1}$. Para obter f^{-1}, devemos trocar as variáveis, y por x e x por y, obtendo assim a nova expressão $x = \frac{5y+2}{3y-1}$. Em seguida, resolvemos essa nova expressão e isolamos a variável y como segue adiante:*

$$x(3y-1) = 5y+2 \Rightarrow 3xy - x = 5y+2 \Rightarrow 3xy - 5y = x+2 \Rightarrow y(3x-5) = x+2 \Rightarrow y = \frac{x+2}{3x-5}.$$

Portanto, a função inversa da $f(x)$ é a função $f^{-1}(x) = \frac{x+2}{3x-5}$.

Assim, abordou-se neste capítulo, uma breve contextualização histórica sobre a evolução do conceito de função e também foi feito um estudo sobre funções, em particular, funções afins. Apresentou-se também, as definições de outras funções como, por exemplo, as definições das funções injetoras, sobrejetoras, bijetoras e funções inversas, uma vez que essas definições serão necessárias para estabelecer uma conexão entre a criptografia e funções que será apresentada no próximo capítulo.

4 CRIPTOGRAFIA E FUNÇÕES

Foi abordada no capítulo 2, uma breve contextualização a respeito da criptografia e sua relevância e, logo em seguida, no capítulo 3, falamos um pouco sobre a evolução do conceito de função e nos concentramos mais especificamente ao estudo das funções afins, injetoras, sobrejetoras, bijetoras e finalmente sobre as funções inversas.

Nesse capítulo, iremos fazer uma ligação entre criptografia e funções, salientando, assim, que a criptografia pode ser inserida dentro do conteúdo das funções, bem como dentro de outros conteúdos pertinentes ao Ensino Fundamental da Educação Básica.

A proposta de inserir a criptografia juntamente ao conteúdo de funções para alunos do 9^o ano do Ensino Fundamental está relacionada com a necessidade de buscar novos meios para promover aulas diversificadas e contextualizadas, proporcionando aos alunos novas experiências de aprendizagem.

> 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. 46).

Pereira (2015, p. 13) diz que "a criptografia aborda temas em diferentes níveis do processo de ensino e aprendizagem, além de propiciar a interdisciplinaridade com as áreas de códigos e linguagem bem como a área de humanas". Ainda para Pereira (2015), a criptografia se relaciona com essas áreas de códigos e linguagem, por exemplo, em uma decifragem por análise de frequência, é necessário um conhecimento profundo da própria linguagem, assim como a análise da frequência com que as letras aparecem no alfabeto, as palavras e pronomes mais utilizados promovem a ligação entre essas áreas e a criptografia. Assim, percebemos que o tema criptografia está em conformidade com os PCNs.

> O critério central é o da contextualização e da interdisciplinaridade, ou seja, é o potencial de um tema permitir conexões entre diversos conceitos matemáticos e entre diferentes formas de pensamento matemático, ou, ainda, a relevância cultural do tema, tanto no que diz respeito às suas aplicações dentro ou fora da Matemática, como a sua importância histórica no desenvolvimento da própria ciência (BRASIL, 2002, p. 43).

Para Borges (2008), a criptografia pode ser inserida em várias áreas e níveis de conhecimento, logo suas aplicações podem partir do conteúdo do Ensino Fundamental e chegar aos maiores problemas da atualidade. Além de sua capacidade para contribuir com o melhoramento do ensino de Matemática, a criptografia é capaz de despertar a curiosidade e aguçar a imaginação dos alunos, provavelmente por estar lidando com segurança, seja

de uma simples conversa pelo Whatsapp, ou mesmo ao enviar um e-mail pessoal, bem como executar transações financeiras de uma grande instituição.

4.1 Trabalhos relacionados ao tema criptografia e funções

Com a finalidade de agregar ao embasamento necessário para o desenvolvimento desse trabalho, foi feito levantamento bibliográfico relacionado ao tema abordado (criptografia e funções). Dentre vários trabalhos encontrados e analisados, alguns serviram como referencial devido a sua conformidade com a presente pesquisa. Nessa percepção, podemos destacar os trabalhos de Nádia Marques Ikeda Pereira (PEREIRA, 2015), o de Beatriz Fernanda Litoldo (LITOLDO, 2016) e o trabalho de Silvana Leal da Silva, Ramon Chagas Santos e Karina França Bragança (SILVA; SANTOS e BRAGANÇA, 2017).

4.1.1 Criptografia: uma nova proposta de ensino de Matemática no ciclo básico

O trabalho de Pereira (2015) é uma dissertação de mestrado intitulada "Criptografia: uma nova proposta de ensino de Matemática no ciclo básico", defendida em 2015, em que a criptografia é evidenciada como instrumento enriquecedor no ensino da Matemática.

Em seu trabalho, Pereira (2015) relata alguns aspectos históricos relacionados à criptografia bem como apresenta a Matemática necessária para o seu desenvolvimento. Em sua pesquisa, Pereira (2015) faz uma associação da criptografia com temas pertinentes à grade curricular do Ensino Médio e dos anos finais do Ensino Fundamental, como funções e números primos.

Sua pesquisa evidencia que o tema criptografia pode ser usado como ferramenta para enriquecer o ensino da Matemática, pois sua aplicabilidade abrange os diferentes níveis de ensino e auxilia no desenvolvimento de competências de leitura e escrita por meio da história, além de colaborar com a interdisciplinaridade e principalmente tornar o aprendizado mais significativo.

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

Outro trabalho que contribuiu para o desenvolvimento dessa pesquisa foi a dissertação denominada "As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim", de autoria de Beatriz Fernanda Litoldo (LITOLDO, 2016), cujo objetivo era compreender como a criptografia poderia auxiliar os alunos na exploração das ideias associadas à função afim.

Em sua pesquisa, Litoldo (2016) elaborou uma sequência de atividades pedagó-

gicas contendo problemas criptográficos com a intenção de abordar a definição de função afim e suas particularidades tais como a função linear, identidade e constante. Também foi abordada em sua pesquisa a representação gráfica dessas funções e a definição da função inversa. Por fim, Litoldo (2016) conclui que os alunos desenvolveram atitudes autônomas durante o processo de aprendizagem adquirindo posturas investigativas. Assim pode concluir que 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.

4.1.3 Criptografia: Uma ferramenta para o estudo de função afim e de sua inversa

Um terceiro trabalho, também importante na construção das ideias para a conclusão da presente pesquisa, foi o trabalho intitulado "Criptografia: Uma ferramenta para o estudo de função afim e de sua inversa." (SILVA; SANTOS e BRAGANÇA, 2017).

O objetivo desse trabalho foi investigar as contribuições da criptografia no processo de ensino aprendizagem de função afim e de sua inversa no Ensino Médio. Com a finalidade de que tal objetivo fosse alcançado, elaborou-se uma sequência didática dividida em três momentos.

No primeiro momento, foi feita uma sondagem para verificar o conhecimento dos alunos em relação ao tema abordado. Já, no segundo momento, desenvolveu-se um estudo sobre a criptografia e suas relevâncias e, em seguida, apresentou-se a relação estabelecida entre criptografia e a função afim e sua inversa. Finalmente foi feita uma intervenção pedagógica para detalhar as etapas realizadas, avaliando-as e produzindo explicações que sejam capazes de justificar seus efeitos, fundamentadas nos dados obtidos e nas teorias adotadas com fundamentação do trabalho.

É uma pesquisa de caráter qualitativo que buscou tornar a aprendizagem de função afim e sua inversa significativa, por meio da contextualização proporcionada pela criptografia.

4.2 Análise dos trabalhos relacionados ao tema criptografia e funções

O trabalho de Nádia Marques Ikeda Pereira procura evidenciar a criptografia como uma forma de enriquecer o ensino da Matemática e, procura associar os conceitos matemáticos, em aplicações que envolva o cotidiano dos educandos, para tornar o aprendizado mais significativo.

Já o trabalho de Beatriz Fernanda Litoldo busca compreender em que atividades envolvendo problemas de criptografia podem auxiliar os alunos na exploração das ideias associadas à função afim. Em seu trabalho, a maneira que ela apresentou para alcan-

çar o objetivo, foi desenvolver atividades estruturadas na forma de contos baseados no personagem Sherlock Holmes, de sir Arthur Conan Doyle.

Finalmente, Silvana Leal da Silva, Ramon Chagas Santos e Karina França Bragança em sua pesquisa, procuram investigar as contribuições da criptografia no processo de ensino e aprendizagem da função afim e sua inversa. Um dos objetivos específicos do trabalho é possibilitar que a aprendizagem de função afim e de sua inversa seja significativa para o aluno utilizando a interdisciplinaridade existente entre a criptografia e a Matemática.

Portanto, existe uma relação entre os objetivos apresentados nos três trabalhos, uma vez que buscam aplicar a criptografia como ferramenta para enriquecer, auxiliar e investigar meios que facilitam a aprendizagem da função afim.

No processo de elaboração destes trabalhos, provavelmente um dos desafios enfrentados deve ter surgido ao tentar promover o entendimento da criptografia para os estudantes, uma vez que este tema não faz parte das disciplinas corriqueiras. A escolha do tema para estabelecer a conexão com a criptografia também deve ter sido crucial para o desenvolvimento dos trabalhos.

A partir daí, várias estratégias foram estabelecidas, cada autor com a sua em particular, procurando construir uma ligação entre os dois temas. Assim, cada um com sua idealização, puderam colocar em prática suas técnicas visando seus objetivos e dessa forma concluir suas pesquisas. Foi a partir dessas estratégias que surgiu a ideia que constitui a base dessa dissertação.

Ao concluir essas análises e ter verificado cada uma das táticas apresentadas, surgiu então a ideia de fazer a relação entre criptografia e função. Quando se fala em criptografia, é natural que a maioria dos alunos desconheça suas aplicações e utilidades, no entanto, no decorrer das explicações, quando se fala da necessidade de obter a segurança nos meios de comunicação, desperta uma certa curiosidade e o interesse pelo tema. A partir desse momento, é hora de esclarecer de que forma a criptografia nos protege e como ela está presente em nossas vidas.

Naturalmente, no decorrer das explicações, vão surgindo os conceitos como codificar e decodificar. Esse é o momento ideal para reforçar os conceitos de função e mostrar a relação existente com a criptografia, uma vez que, para fazermos uma codificação, poderemos usar uma determinada função e, para desfazermos esse processo, ou seja, decodificar, será necessário usar a inversa dessa função. Esse processo constitui a base dessa pesquisa e será mostrado mais detalhadamente no próximo capítulo.

5 PROPOSTA DA PESQUISA

Após reunir todas as informações adquiridas ao longo do desenvolvimento dessa pesquisa, pretendeu-se criar um meio para auxiliar o aprendizado do conteúdo de funções. Espera-se também que esse mecanismo proporcione uma aprendizagem com significado para o aluno e viabilize aulas diversificadas e atraentes, vinculando os saberes matemáticos escolares às situações cotidianas dos educandos, tendo como ferramenta principal a criptografia.

> Cabe, portanto, ao ensino de Matemática garantir que o aluno adquira certa flexibilidade para lidar com o conceito de função em situações diversas e, nesse sentido, através de uma variedade de situações problema de Matemática e de outras áreas, o aluno pode ser incentivado a buscar a solução, ajustando seus conhecimentos sobre funções para construir um modelo para interpretação e investigação em Matemática (BRASIL 2002, p. 44).

5.1 A escolha do tema

A ideia de se trabalhar com a criptografia ocorreu devido ao fato desse tema estar sendo amplamente utilizado nos meios digitais hoje em dia e de seu potencial para estabelecer ligações entre diversas áreas e níveis de conhecimento. Com o crescimento tecnológico, houve uma invasão virtual na rotina diária das pessoas, principalmente por meio de celulares e computadores, pois atualmente vivemos em um mundo cada vez mais digital e globalizado.

Por outro lado, o estudo de função é importante na construção dos saberes matemáticos e, seu conhecimento não é restrito apenas aos interesses da Matemática.Suas aplicações são recorrentes no cotidiano dos alunos, portanto, uma conexão entre a criptografia e funções surtiria efeitos positivos para a aprendizagem.

> A criptografia é um tema atual que possibilita o desenvolvimento de atividades didáticas (Tamarozzi, 2001), que podem ser desenvolvidas no Ensino Fundamental, que levem os alunos a aprimorarem seus conhecimentos, levando-os a adquirirem as habilidades e competências de resolver problemas, criar estratégias de resolução, autonomia durante o processo de aprendizagem, com isso, tornando-os mais autoconfiantes e concentrados na realização das atividades e buscando interligar os conteúdos matemáticos às situações do mundo real (GROENWALD e FRANKE, 2008 apud GROENWALD e OLGIN, 2010).

Grande parte das pessoas passa bom tempo de suas vidas conectadas a computadores e celulares, usando esses aparelhos para fazerem praticamente tudo (transferências eletrônicas, pagamento de contas, compras, aluguel de filmes, contratam funcionários, monitoram filhos, casas, estabelecimentos, etc.). Enfim, o controle está na palma das mãos.

No entanto, por trás de tanta comodidade, informações trafegam a todo tempo levando e trazendo todo tipo de conteúdo para suprir essas necessidades tecnológicas,

cada vez mais presentes e atualmente indispensáveis para a maioria das pessoas. Contudo, tantas informações circulando livremente, contendo segredos pessoais, informações governamentais e até mesmo sigilos militares, necessitam de uma determinada segurança para proteger seus usuários. Essa segurança, que estamos referindo, está relacionada com a criptografia.

Por outro lado, quando se fala em ensino e aprendizagem, provavelmente um dos maiores desafios enfrentados pelos professores de Matemática, está relacionado com a falta de interesse pela matéria apresentada por parte dos alunos. Normalmente, as aulas de Matemática são ministradas por uma metodologia tradicional com ênfase excessiva no cálculo, direcionado a uma incansável resolução de exercícios, que induz a uma mera repetição do que foi visto em sala de aula. Outro agravante é a falta de contextualização e a linguagem utilizada. Dessa maneira, as aulas acabam se tornando desagradáveis e desgastantes, levando parte dos estudantes a perder o interesse pelo conteúdo.

> Infelizmente, os resultados obtidos com a metodologia tradicional (conceituação, seguida de exercícios de manipulação, com algumas aplicações) não têm sido satisfatórios, por várias razões. Frequentemente, o material teórico é apresentado como uma simples lista de fatos e fórmulas, às vezes sem qualquer justificativa, que o aluno, então, memoriza através de exercícios repetitivos. As aplicações, por sua vez, na maior parte das vezes, são divorciadas da realidade, ou pelo menos da realidade dos alunos, frustrando o objetivo de mostrar a relevância da Matemática para as aplicações. O resultado é uma Matemática em que os alunos raciocinam muito pouco: o que eles mais fazem é aplicar mecanicamente determinados procedimentos rotineiros (CARVALHO, 2005, p. 13).

O professor, para não perder o direcionamento de seu trabalho e retomar a atenção desejada, deve buscar meios para mudar essa situação. Assim, procurar diversificar as atividades, selecionar os exercícios abordados, promover atividades que envolvam situações vivenciadas por seus alunos e trazer para sala de aula, temas que podem provocar o entusiasmo pela matéria, são alternativas que podem ser exploradas pelo professor.

Nesse contexto, surge então o projeto de inserir a criptografia juntamente com o conteúdo de funções. Assim, a criptografia será o instrumento motivador para despertar no educando, o interesse pela Matemática, vivenciando em sala de aula, experiências concernentes a sua rotina. Motivar é contribuir de forma significativa no sentido de tornar essas experiências mais interessantes, assim, a criptografia será ferramenta fundamental para motivar o estudo de funções.

Dessa forma, essa pesquisa visa possibilitar resultados satisfatórios ao tornar as aulas mais dinâmicas, motivadoras e promover, ao aluno, métodos para fixar, exercitar, aprofundar e revisar esses conteúdos.

> Para as instâncias educacionais (professores, escolas, secretarias, etc.) impõe-se uma discussão pedagógica permanente sobre como a Matemática se insere no contexto da educação. Um desafio importante nessa discussão é encontrar soluções que possam oferecer um ensino de Matemática

> de qualidade para todos, sem que para isso seja necessário impor à maioria dos alunos muitos conteúdos que não tenham um sentido mais objetivo em suas vidas. Essa não é uma discussão para poucas pessoas - é tarefa de todos os professores que, de alguma forma, estejam ligados ao ensino na área de Matemática, seja atuando em sala de aula, seja colaborando na formação de currículos e diretrizes ou, ainda, produzindo livros e material didático (DRUCK, 2005, p. 3-4).

5.2 Metodologia utilizada em sala de aula

Organizou-se esse trabalho com o propósito de elaborar aulas atraentes, diversificadas e contextualizadas para incitar nos estudantes o entusiasmo em aprender a Matemática e despertar o interesse pelo conteúdo de funções, em particular, funções afins. Assim, a criptografia foi inserida como instrumento motivador ao conteúdo de funções para alunos do 9º ano do Ensino Fundamental. A princípio, desenvolveu-se um estudo bibliográfico acerca do tema criptografia, em que foi feita uma contextualização histórica e suas relevâncias. Em seguida, também foi feito um estudo sobre função afim, função injetora, função sobrejetora, função bijetora e função inversa, bem como a relação entre os dois temas, criptografia e funções.

Em um segundo momento, foi feita uma pesquisa de caráter qualitativo que teve como instrumentos de coleta de dados a observação direta, aplicação de pré-teste e pós-teste e respostas das atividades propostas.

> 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 apud SILVA; SANTOS e BRAGANÇA, 2017, p. 42).

Gil (2002, p. 115) diz que "Analisando-se cada uma das três técnicas, pode-se verificar que o questionário constitui o meio mais rápido e barato de obtenção de informações, além de não exigir treinamento de pessoal e garantir o anonimato." Através do pré-teste, pôde-se traçar o perfil dos alunos e identificar os seus conhecimentos acerca dos temas criptografia e funções.

> 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" (SILVA; SANTOS e BRAGANÇA, 2017, p. 42).

As atividades foram desenvolvidas com alunos do 9^o ano do Ensino Fundamental do Colégio Visão, em Formosa-Goiás. O Colégio Visão é considerado referência em educação na cidade de Formosa, pertence à rede particular de ensino e está localizado na Avenida João Ísper Gebrim, 2.630 – Bairro Formosinha, Formosa Goiás.

Os alunos participantes foram alunos dos 9^o anos A, B e C que se dispuseram a participar das atividades. Ao todo, foram envolvidos 16 alunos, dos quais, seis homens e dez mulheres com faixa etária entre 13 e 14 anos.

As atividades foram aplicadas em horário contrário ao horário das aulas, sempre às terças-feiras, horário de coordenação. Esses encontros aconteceram das 14h às 15h30min e, as atividades desenvolvidas, são apresentadas conforme tabela 8 abaixo.

Tabela 8 – Cronograma das atividades desenvolvidas

Data	Atividades Desenvolvidas
09/10/2018	▶ Conversa informal com os participantes, para explicar a proposta da pesquisa e, a contribuição dos mesmos nesse processo; ▶ Aplicação do pré-teste (anexo A): atividade para verificação do conhecimento prévio sobre criptografia, função bijetora e função inversa.
16/10/2018	▶ Exposição do tema criptografia e relatos de alguns fatos históricos envolvendo suas aplicações; ▶ Exemplos e atividades para mostrar a criptografia utilizada no bastão de Licurgo e na cifra de César.
23/10/2018	▶ Exposição do tema funções: definição das funções afim, injetora, sobrejetora, bijetora e função inversa; ▶ Mostrar a relação entre criptografia e funções.
30/10/2018	▶ Mostrar como codificar e decodificar mensagens usando as funções afins.
06/11/2018	▶ Aplicação do pós-teste (anexo B): atividade para verificar se os participantes compreenderam os temas e atividades abordados nos encontros anteriores.
13/11/2018	▶ Aplicação da atividade final (anexo C): atividade cuja intenção, era saber a opinião dos participantes em relação ao trabalho de um modo geral.

Fonte: Autor

Após finalizar as atividades desenvolvidas, foi feita uma análise dos dados coletados no pré-teste, com os resultados obtidos com a aplicação do anexo B. Portanto, com essa análise, pretende-se verificar se os objetivos foram alcançados. Os detalhes dessa análise são apresentados na próxima seção.

Salienta-se ainda que o autor da pesquisa estava na condição de professor regente dessas turmas de 9^o ano e, nesse período, ministrava o conteúdo de funções para as turmas mencionadas. Assim, foi possível a observação direta dos alunos e do conteúdo que estava sendo abordado.

5.3 Relato das atividades desenvolvidas

5.3.1 Aplicação do pré-teste (anexo A)

O início das atividades ocorreu com a realização do anexo A, no dia 09 de outubro de 2018. Este anexo representa um pré-teste e foi aplicado para os dezesseis alunos voluntários das três turmas de 9^o ano do Ensino Fundamental, do Colégio Visão, em Formosa-Goiás, que se prontificaram para compor o corpus da pesquisa. Esse pré-teste teve a finalidade de investigar o conhecimento desses alunos acerca dos temas criptografia, função bijetora e função inversa.

Para verificar o conhecimento dos participantes sobre os temas, o anexo A continha cinco questões abertas, em que o aluno tinha liberdade de expressar, com suas próprias palavras, o que sabia a respeito do tema.

Figura 20 – Aplicação do pré-teste, registro de pesquisa

Fonte: Autor

Após a aplicação do teste, verificou-se que a maioria dos estudantes possivelmente não conseguiriam responder a todas às perguntas.

5.3.2 Encontros para expor o tema da pesquisa

Após a realização do pré-teste, foi agendado o segundo encontro. Nesse encontro, expôs-se o objetivo da pesquisa e qual seria a contribuição dos participantes nesse processo. Explicou-se, com detalhes, o significado da palavra criptografia, qual sua função e também qual sua importância para a sociedade ao longo da história. Assim, foi feito um levantamento histórico sobre o tema, destacando fatos imprescindíveis para o desenvolvimento da criptografia.

Atividades também foram desenvolvidas em uma roda de conversa para mostrar o funcionamento do bastão de Licurgo, sistema utilizado pelos espartanos por volta de

475 a.C., tornando-se o primeiro aparelho criptográfico militar. A *cifra de César* chamou atenção dos alunos, que ficaram admirados com as mensagens que eles mesmos cifraram e também decifraram, simplesmente pelo deslocamento de determinadas letras. Comentou-se também que este sistema criptográfico permaneceu indecifrável por muito tempo e só mais adiante que ele seria facilmente decifrado com a análise de frequência das letras. A frequência das letras no alfabeto português foi mostrada para os participantes, bem como o método para decifrar uma mensagem cifrada com a *cifra de César*, sem conhecer o deslocamento utilizado. A tabela 9 a seguir, mostra o percentual de frequência de letras em uma análise de textos escrito no idioma português.

Tabela 9 – Percentual de frequência de letras no português

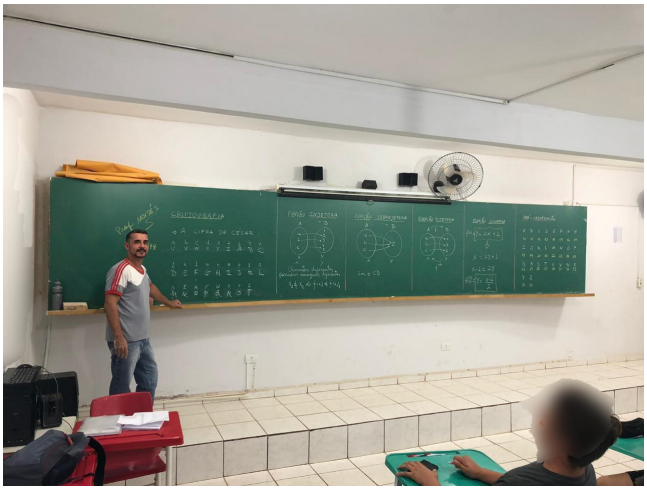
Letra	Frequência	Letra	Frequência
A	14,64%	N	5,05%
B	1,04%	O	10,73%
C	3,88%	P	2,52%
D	4,10%	Q	1,20%
E	12,57%	R	6,53%
F	1,02%	S	7,81%
G	1,30%	T	4,34%
H	1,28%	U	4,64%
I	6,18%	V	1,70%
J	0,40%	W	0,01%
K	0,02%	X	0,21%
L	2,78%	Y	0,01%
M	4,75%	Z	0,47%

Fonte: Coutinho (2015) adaptado pelo autor

Em nosso terceiro encontro, foram abordados os conceitos de função injetora e função sobrejetora com o propósito de obter condições para o entendimento da função bijetora e, consequentemente da existência da função inversa. Nesse encontro, também foram feitas várias atividades para identificar se uma dada função era injetora, sobrejetora ou bijetora e também atividades para determinar a inversa de uma função afim qualquer. Ainda nessa aula, munidos dos conhecimentos adquiridos sobre criptografia, função bijetora e função inversa, pôde-se relacionar o tema criptografia com funções.

O quarto encontro foi especial, pois, neste encontro, mostrou-se que a criptografia poderia ser inserida no conteúdo que estávamos trabalhando em sala de aula. Isso tornou o encontro mais interessante, pois os alunos já tinham um conhecimento básico sobre a criptografia por meio dos encontros anteriores e estavam ansiosos para saberem como aplicá-la em algo que eles já estavam estudando, ou seja, as funções.

Figura 21 – Encontros para expor o tema da pesquisa - registro de pesquisa



Fonte: Autor

Os estudantes já sabiam como cifrar e decifrar mensagens usando a *cifra de César*, agora eles estavam curiosos para saberem como codificar e decodificar mensagens usando funções.

A aplicação de funções afins, para codificar e decodificar mensagens, que será abordada nessa seção, não é a mesma mostrada na seção 2.6 do capítulo 2 sobre o sistema RSA. A escolha desse método foi devido ao fato de ser mais fácil, para os alunos, o seu entendimento.

A ideia foi mostrada seguindo as etapas a seguir:

- Em primeiro lugar, montamos um quadro pré-codificado com o valor numérico de cada letra do alfabeto. Escolhemos esse valor numérico, de modo arbitrário, porém, é conveniente fazer cada letra corresponder a um número de dois algarismos para evitar confusões, pois, se fizéssemos, a letra A corresponder ao número 1, a letra B corresponder ao número 2 e assim por diante, o número 11 poderia representar AA ou K, que é a décima primeira letra do alfabeto e o número 12 poderia representar AB ou L, que é a décima segunda letra do alfabeto, e dessa forma, não teríamos como decidir qual a escolha correta. Portanto, para evitar ambiguidades, é conveniente fazer cada letra corresponder a números com a mesma quantidade de algarismos. Assim, representamos cada letra por um número de dois algarismos como mostra a tabela 10:

Tabela 10 – Pré-codificação com o valor numérico de cada letra do alfabeto

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: Autor

- Em seguida, escolhemos a função afim $y = 3x - 2$ e a representamos por $c(x) = 3x - 2$ para indicar que essa será a função codificadora;
- A frase **"ESTUDAR É BOM"** foi escolhida para fazer a codificação;
- A partir da pré-codificação apresentada na tabela 10, substituímos cada letra da frase pelo número que a representa na tabela, ou seja,

$$E = 14, S = 28, T = 29, U = 30, D = 13, A = 10, R = 27, B = 11, O = 24 \text{ e } M = 22.$$

Assim, a frase **"ESTUDAR É BOM"** foi pré-codificada como **"14282930131027 14 112422"**.

- Usamos a função codificadora $c(x) = 3x - 2$ para codificar a mensagem pré-codificada **"14282930131027 14 112422"**. Dessa forma, obtivemos:

$$E = 14 \Rightarrow c(14) = 3.14 - 2 \Rightarrow c(14) = 42 - 2 \Rightarrow c(14) = 40.$$

Portanto, a letra E, codificada pela função $c(x)$, foi representada pelo número 40, isto é, E = 40. Desse modo, o restante da frase foi codificada, seguindo o mesmo procedimento.

$S = 28 \Rightarrow c(28) = 3.28 - 2 \Rightarrow c(28) = 84 - 2 \Rightarrow c(28) = 82 \Rightarrow A$ codificação de S é 82
$T = 29 \Rightarrow c(29) = 3.29 - 2 \Rightarrow c(29) = 87 - 2 \Rightarrow c(29) = 85 \Rightarrow A$ codificação de T é 85
$U = 30 \Rightarrow c(30) = 3.30 - 2 \Rightarrow c(30) = 90 - 2 \Rightarrow c(30) = 88 \Rightarrow A$ codificação de U é 88
$D = 13 \Rightarrow c(13) = 3.13 - 2 \Rightarrow c(13) = 39 - 2 \Rightarrow c(13) = 37 \Rightarrow A$ codificação de D é 37
$A = 10 \Rightarrow c(10) = 3.10 - 2 \Rightarrow c(10) = 30 - 2 \Rightarrow c(10) = 28 \Rightarrow A$ codificação de A é 28
$R = 27 \Rightarrow c(27) = 3.27 - 2 \Rightarrow c(27) = 81 - 2 \Rightarrow c(27) = 79 \Rightarrow A$ codificação de R é 79
$B = 11 \Rightarrow c(11) = 3.11 - 2 \Rightarrow c(11) = 33 - 2 \Rightarrow c(11) = 31 \Rightarrow A$ codificação de B é 31
$O = 24 \Rightarrow c(24) = 3.24 - 2 \Rightarrow c(24) = 72 - 2 \Rightarrow c(24) = 70 \Rightarrow A$ codificação de O é 70
$M = 22 \Rightarrow c(22) = 3.22 - 2 \Rightarrow c(22) = 66 - 2 \Rightarrow c(22) = 64 \Rightarrow A$ codificação de M é 64

Finalmente, a frase **"ESTUDAR É BOM"**, pôde ser codificada como

"40828588372879 40 317064".

- Depois fizemos a decodificação da mensagem **"40828588372879 40 317064"**. Para isso, calculamos a função inversa de $y = 3x - 2$, explicado no terceiro encontro. Sua inversa foi obtida trocando-se as variáveis y por x e x por y, assim, obtivemos a nova expressão $x = 3y - 2$. Em seguida, isolamos a variável y, isto é,

$$3y = x + 2 \Rightarrow y = \frac{x+2}{3},$$

e a representamos por $d(x) = \frac{x+2}{3}$ para indicar que essa será a função decodificadora;

- Usamos a função decodificadora $d(x) = \frac{x+2}{3}$, para decodificar a mensagem codificada **"40828588372879 40 317064"**. Dessa forma,

$$d(40) = \frac{40+2}{3} \Rightarrow d(40) = \frac{42}{3} \Rightarrow d(40) = 14.$$

Portanto, o número 14, representa a letra E, decodificada pela função $d(x)$ usando a tabela 9, isto é, $14 = E$. Assim, o restante da frase foi decodificada, seguindo o mesmo procedimento e, obtemos:

$$d(82) = \frac{82+2}{3} \Rightarrow d(82) = \frac{84}{3} \Rightarrow d(82) = 28 = S;$$

$$d(85) = \frac{85+2}{3} \Rightarrow d(85) = \frac{87}{3} \Rightarrow d(85) = 29 = T;$$

$$d(88) = \frac{88+2}{3} \Rightarrow d(88) = \frac{90}{3} \Rightarrow d(88) = 30 = U;$$

$$d(37) = \frac{37+2}{3} \Rightarrow d(37) = \frac{39}{3} \Rightarrow d(37) = 13 = D;$$

$$d(28) = \frac{28+2}{3} \Rightarrow d(28) = \frac{30}{3} \Rightarrow d(28) = 10 = A;$$

$$d(79) = \frac{79+2}{3} \Rightarrow d(79) = \frac{81}{3} \Rightarrow d(79) = 27 = R;$$

$$d(40) = \frac{40+2}{3} \Rightarrow d(40) = \frac{42}{3} \Rightarrow d(40) = 14 = E;$$

$$d(31) = \frac{31+2}{3} \Rightarrow d(31) = \frac{33}{3} \Rightarrow d31) = 11 = B;$$

$$d(70) = \frac{70+2}{3} \Rightarrow d(70) = \frac{72}{3} \Rightarrow d(70) = 24 = O;$$

$$d(64) = \frac{64+2}{3} \Rightarrow d(64) = \frac{66}{3} \Rightarrow d(64) = 22 = M.$$

Portanto, a frase codificada **"40828588372879 40 317064"**, significa **"ESTUDAR É BOM"**, que foi decodificada usando a função decodificadora $d(x)$.

5.3.3 Aplicação do pós-teste (anexo B)

O quinto encontro foi marcado pela expectativa dos participantes. Foi o momento de colocar em prática o que foi visto nos encontros anteriores, ou seja, foi o momento de avaliar as atividades.

O anexo B continha duas atividades. A atividade 1 era para decifrar uma mensagem cifrada com a *cifra de César*. Nessa atividade, os alunos teriam que usar a análise de frequência das letras no alfabeto português para identificar qual seria o deslocamento utilizado. A utilização dos percentuais de frequência de letras no alfabeto português, usado para decifrar uma mensagem, foi uma técnica explicada nos encontros anteriores. Essa técnica, consiste em observar as letras que mais aparecem em uma mensagem codificada, para relacioná-las com as letras de maior frequência no alfabeto utilizado e, desse modo, tentar descobrir o deslocamento utilizado na codificação da mensagem. A atividade 2, ocorre entre dois indivíduos A e B. O indivíduo A deveria enviar a mensagem codificada e o indivíduo B teria que decodificar a mensagem. Nessa atividade foi dada a função codificadora $c(x) = 2x - 9$ e, na primeira questão, os participantes teriam que obter a sua inversa chamada de $d(x) = \frac{x+9}{2}$. Na segunda questão, eles teriam que decodificar uma mensagem usando a função inversa $d(x)$. Na terceira questão, foi pedido para fazer uma codificação a partir da função $c(x)$ e, finalmente, na última questão da atividade 2, foi pedido para explicar a condição de existência da função inversa $d(x)$.

5.3.4 Aplicação da atividade final (anexo C)

O nosso sexto e último encontro foi finalizado com a aplicação da atividade final (anexo C). O anexo C foi elaborado com dez questões fechadas, cuja finalidade era verificar a opinião de cada participante a respeito do tema central que estava definido em seu enunciado, a saber: "A ideia essencial no desenvolvimento desse trabalho é estabelecer uma relação entre uma situação recorrente aos alunos com os conteúdos matemáticos trabalhados em sala de aula, além de contemplá-los com a novidade do tema. Nessa perspectiva, a criptografia foi inserida como instrumento motivador, para enriquecer o ensino de funções afins no 9º ano do Ensino Fundamental. Com base no que está sendo proposto, responda as perguntas a seguir".

As questões do anexo C versavam sobre a importância da criptografia, se a ligação entre criptografia e funções foi interessante, se o tema função bijetora e função inversa foi relevante, o que eles acharam da ideia central do trabalho e qual era a opinião deles em relação à pesquisa de um modo geral.

Portanto, o anexo C finalizou a série de seis encontros em que se explorou desde a definição da palavra criptografia até a sua importância nos dias de hoje e mostrou também como o tema é abrangente e que sua aplicação pode proporcionar um crescimento

positivo em relação à aprendizagem em sala de aula.

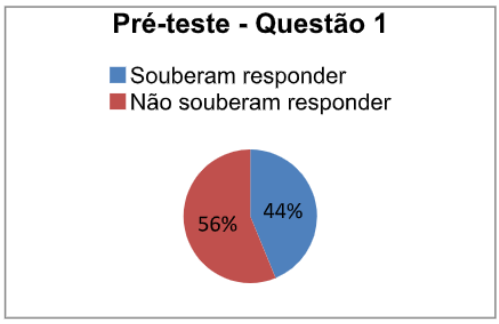
5.3.5 Análise dos dados coletados no pré-teste e comparação com os dados coletados no pós-teste (anexo B) para verificar se os objetivos foram alcançados.

A título de exemplo, apresentamos as perguntas do anexo A.

Questão 1 - Você sabe o que é criptografia?

O percentual dos alunos que disseram saber o que é criptografia é dado no gráfico na figura 22.

Figura 22 – Percentual da questão 1



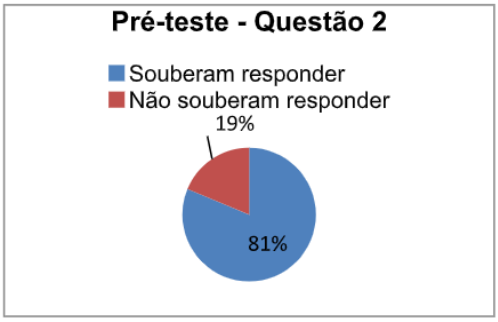
Fonte: Autor

Nessa questão, prevaleceram respostas curtas, sem justificativas, como "*sim*" ou "*não*". E o restante das respostas, apresentou justificativas diversas. A que mais chamou atenção foi "*É uma forma de esconder mensagens ou dados por meio de alguma 'chave', tipo código morse ou binário*".

Abaixo, é apresentado o percentual dos alunos que disseram saber responder as outras quatro questões que compunham o pré-teste, bem como, uma breve análise das respostas de cada questão.

Questão 2 - A criptografia está presente em nosso cotidiano. Você conhece ou sabe de algum aparelho onde ela está sendo utilizada?

Figura 23 – Percentual da questão 2

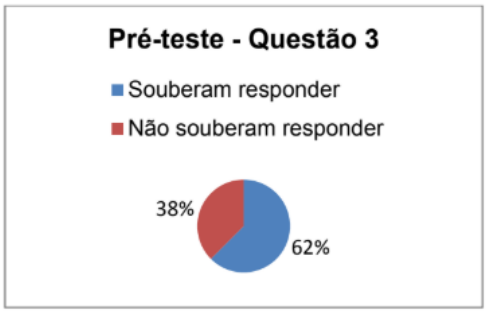


Fonte: Autor

Nessa questão, predominaram respostas como "*celulares*", "*computadores*" e "*aplicativos de whatsapp*". Também houve um número pequeno de respostas como "*sim*" ou "*não*" sem justificativas.

Questão 3 - Você sabe dizer para que serve a criptografia?

Figura 24 – Percentual da questão 3

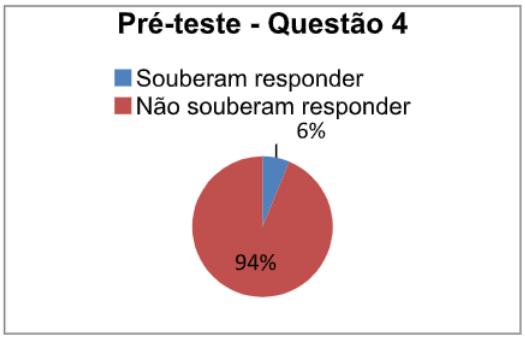


Fonte: Autor

As respostas prevalecentes nessa questão foram "*proteção*" e "*segurança*" e outros seis participantes restantes, responderam apenas "*não*".

Questão 4 - Você sabe o que é uma função bijetora? E uma função inversa, sabe o que é?

Figura 25 – Percentual da questão 4

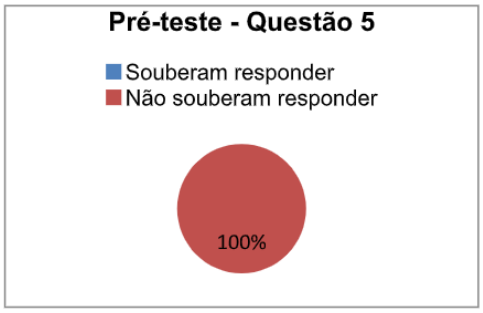


Fonte: Autor

Aqui, as respostas praticamente foram iguais, a maioria respondeu "*não*", "*não sei*", "*não tenho conhecimento sobre o assunto*", "*não sei, mas já ouvi falar*". Apenas um participante respondeu que sabia o que era, porém não fez nenhum comentário.

Questão 5 - Qual é a condição para que uma função admita inversa?

Figura 26 – Percentual da questão 5



Fonte: Autor

Dos dezesseis participantes, onze responderam "*não sei*", dois responderam apenas "*não*", um respondeu "*não tenho conhecimento sobre o assunto*" e dois deixaram a resposta em branco.

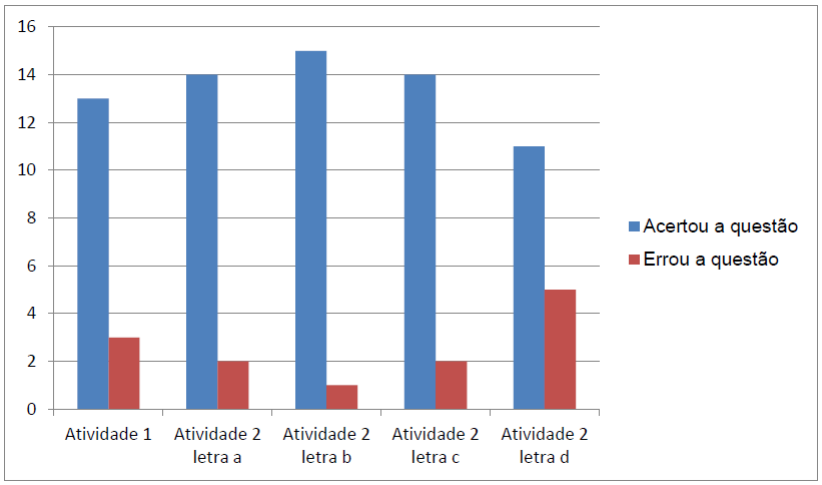
Com o resultado do pré-teste, verificou-se que a maioria dos participantes desconhecia os temas abordados, pois os questionamentos nele contidos se referiam a criptografia, função bijetora e função inversa, temas que não compõem a grade curricular do 9º ano do Ensino Fundamental. Sem dúvida, esse era um dos desafios da pesquisa, isto é, fazer com que uma novidade produzisse um efeito positivo e satisfatório dentro do âmbito escolar.

Após os encontros realizados para expor o tema criptografia e funções, foi feita a aplicação do pós-teste (anexo B) e, nesse momento, os participantes tinham as noções necessárias para debater a respeito dos temas, portanto, a intenção era obter um quadro bem diferente daquele alcançado no pré-teste.

Observou-se, com o pós-teste, que os alunos conseguiram fazer a maioria das atividades e ficaram satisfeitos com a experiência. Puderam fazer a aplicação de conceitos que eles estavam vendo em sala de aula, no caso as funções afins juntamente com a novidade da criptografia. Tiveram a oportunidade de decifrar uma mensagem cifrada com a *cifra de César* usando a análise de frequência das letras do alfabeto português e conseguiram decodificar uma mensagem usando a função inversa de outra função dada e também souberam responder que a existência da função inversa só foi possível por causa da bijeção. A parte que eles tiveram mais dificuldade na primeira atividade, que pedia para decifrar uma mensagem, codificada com a *cifra de César*, foi descobrir o deslocamento utilizado. Porém, foi explicado que a análise de frequência das letras ajudaria a descobrir esse deslocamento utilizado. Outra dificuldade apresentada foi em relação à segunda atividade na letra "a", que pedia para encontrar a função decodificadora, no caso, a função inversa, pois, alguns dos participantes esqueceram a regra para obter a inversa, no entanto, a dica foi dada a eles no momento da aplicação e assim, conseguiram responder

a questão. Essa análise pode ser observada na figura 27 a seguir:

Figura 27 – Número de alunos que acertaram e erraram as atividades do pós-teste (anexo B)



Fonte: Autor

A criptografia era desconhecida por muitos até o primeiro encontro. Quando souberam que se tratava de algo que eles usavam com frequência através de mensagens via whatsapp e computadores, ficaram mais curiosos ainda e se interessaram rapidamente pelo tema. A introdução das funções injetora, bijetora, sobrejetora e também da função inversa fortificou ainda mais o objetivo da pesquisa, pois os participantes descobriram que temas diferentes podem relacionar-se para proporcionar novas experiências que sejam capazes de instigar o entusiasmo pela Matemática e que aulas diferentes e diversificadas não precisam necessariamente de todo um aparato. Algo bem simples e criativo também tem o poder de tornar o ambiente escolar mais agradável e oportuno, fazendo com que os alunos sintam-se motivados com o que está sendo ensinado, alcançando dessa maneira, resultados satisfatórios.

6 CONSIDERAÇÕES FINAIS

Na Educação Básica, em particular, no 9º ano do Ensino Fundamental II, procura-se mostrar para os alunos a importância da Matemática para diversas áreas do conhecimento, além disso, também é conveniente mostrar algumas aplicações do que está sendo tratado. Portanto, o conteúdo de criptografia pode motivar os alunos em sala de aula, em particular, motivar o estudo de funções afins.

Desse modo, houve uma aproximação do cotidiano do aluno por meio da criptografia, uma vez que ela está presente, por exemplo, em mensagens enviadas por celulares, no envio de e-mails e na realização de transações bancárias com os conteúdos trabalhados em sala de aula.

A partir daí, foi elaborada uma estratégia para estabelecer a conexão entre os dois temas e, cujo objetivo, é apresentar a criptografia como uma ferramenta para enriquecer o ensino da Matemática.

A estratégia consistia na explicação do tema e na aplicação de pré-teste e pós-teste para os alunos do 9º ano do Ensino Fundamental do Colégio Visão, em Formosa-Goiás, cuja intensão era destacar os aspectos coesos com os objetivos traçados, bem como os que necessitavam de ajustes. Após a aplicação do pós-teste (anexo B), percebe-se que a metodologia aplicada teve impacto positivo no processo de ensino e aprendizagem.

O pós-teste (anexo C) além de apresentar um resultado positivo quanto à aceitação da proposta da pesquisa em seu conjunto, também deixou explícito a satisfação dos participantes em relação ao método utilizado e aos conteúdos abordados. Com a análise dos dados coletados com a aplicação do anexo C, verifica-se que o objetivo foi alcançado. Assim, por meio desta análise, percebem-se novas possibilidades de aplicações da criptografia como motivação em estudos posteriores, uma vez que esse processo possibilita avanços satisfatórios, tanto no ensino quanto na aprendizagem.

Ademais, além dos resultados positivos em relação aos alunos, este trabalho de conclusão de curso, na verdade o mestrado como um todo, foi norteador na minha prática como docente. Uma vez que ao longo da minha carreira profissional, esse foi um momento ímpar que pude relacionar os meus conhecimentos as situações recorrentes dos alunos e aplicar uma metodologia diferente das que costumava utilizar. Causando desse modo, uma reflexão e um impacto positivo na minha prática docente e consequentemente no ensino.

Assim sendo, a abordagem da criptografia mostrou-se potencialmente motivadora, despertando a curiosidade do aluno e instigando o desejo de aprender. As atividades desenvolvidas são exemplos de recursos didáticos que podem ser utilizados em sala de aula, que têm como objetivos exercitar, aprofundar e revisar o conteúdo de funções.

Nos livros didáticos não se encontra o conteúdo de criptografia e, por esse motivo,

deve-se ir além, ou seja, buscar novidades para sala de aula e, isso pode trazer resultados satisfatórios.

Para novos estudos, é bom salientar que a criptografia, como ferramenta motivadora, também pode ser aplicada a outros conteúdos, tanto no Ensino Fundamental quanto no Ensino Médio, por exemplo, expressões numéricas e equações do 2^o grau envolvendo cartas código, no estudo de outras funções como exponencial e logarítmica, em análise combinatória, matrizes, entre outros.

Neste sentido, a criptografia será uma ferramenta fundamental, pois além de proporcionar ao aluno novas experiências de aprendizagem de forma a considerar as aulas mais desafiadoras, também irá proporcionar uma aprendizagem satisfatória.

REFERÊNCIAS

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de Forma Divertida.** 1. ed. Rio de Janeiro, 2010. 139p.

BORGES, Fabio. **Motivando o Estudo da Matemática através da Criptografia.** In: I Encontro Acadêmico de Modelagem Computacional do Laboratório Nacional de Computação Científica, 2008, Petrópolis/RJ. Resumos. Petrópolis/RJ, 2008. p. 822- 828. Disponível em: < http://www.lncc.br/ borges/doc/Motivando%20o%20Estudo%20da%20Matem%E1tica%20atrav%E9s%20da%20Criptografia.pdf>. Acesso em: 06 de maio 2018.

BRASIL. **Base Nacional Comum Curricular**. Séries Finais do Ensino Fundamental. Brasília: MEC, 2016.

BRASIL. **Parâmetros Curriculares Nacionais**. Terceiro e Quarto Ciclos do Ensino Fundamental, Matemática. Brasília: MEC/SEF, 1998.

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

CARVALHO, Paulo Cezar Pinto. **Fazer Matemática e usar Matemática**. Salto para o futuro. Ministério da Educação, Brasília, DF, Boletim 06, maio 2005. Disponível em: <https://tvescola.org.br/tve/salto-acervo/home>. Acesso em: 25 set. 2018.

CORREIA, José Manuel Teixeira. **A Evolução do Conceito de Função na Segunda Metade do século XVIII.** 1999. 88 f. Tese (Mestrado em Ensino da Matemática) – Departamento de Matemática Pura, Faculdade de Ciências da Universidade do Porto, Universidade do Porto, Cidade do Porto, 1999.

COUTINHO, Severino Collier. **Criptografia.** 1. ed. Rio de Janeiro: IMPA, 2015. 217 p.

COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA.** 2. ed. Rio de Janeiro: IMPA, 2013. 226p. (Coleção Matemática e Aplicações)

CRYPTO, Museum. **Crypto Museum website by Paul Reuvers and Marc Simons.** Disponível em: <http://cryptomuseum.com/mission.htm >. Acesso em: 04 set. 2018.

DRUCK, Suely. **Matemática não é Problema.** Salto para o futuro. Ministério da Educação, Brasília, DF, Boletim 06, maio 2005. Disponível em: <https://tvescola.org.br/tve/salto-acervo/home>. Acesso em: 25 set. 2018.

FERRONI, Marcelo. **Quebrando Códigos:** De Xerxes a Blaise de Vigenère. Disponível em: < http://galileu.globo.com/edic/118/eureca.htm>. Acesso em 25 jul. 2018.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa.** 4. ed. São Paulo: Atlas S.A., 2002. 176p.

GROENWALD, C. L. O.; OLGIN, C. de A. **Códigos e Senhas:** Sequência didática com o tema criptografia no Ensino Fundamental. In: X Encontro Nacional de Educação Matemática, 2010, Salvador BA, Anais. Salvador, 7 jul. 2010. 10p.

HEFEZ, Abramo. **Aritmética.** 1. ed. Rio de Janeiro: SBM, 2014. 338p. (Coleção PROFMAT).

IEZZI, G.; MURAKAMI, C. **Fundamentos de Matemática Elementar:** Conjuntos Funções. 3. ed. São Paulo: Atual Editora, 1977. 164p.

JASPER, Nichols Aron. **História, Técnicas e Classificação de Algoritmos Estenográficos.** 2009. 96 f. Monografia (Tecnólogo em Processamento de Dados) – Faculdade de Tecnologia de São Paulo, FATEC-SP, São Paulo, 2009.

KRISCHER, Thais Cristiane. **Um estudo da máquina Enigma.** 2013. 98 f. Monografia (Graduação em Ciência da Computação) – Bacharelado em Ciência da Computação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2013.

KAHN, David. **The Codebreakers:** The story of secret writing. 1 ed. New York: The New American Library, 1973.

LIMA, Elon Lages. **Números e Funções Reais.** 1. ed. Rio de Janeiro: SBM, 2014. 297p. (Coleção PROFMAT).

LITOLDO, Beatriz Fernanda. **As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função**

afim. 2016. 202 f. Dissertação (Mestrado em Educação Matemática) – Instituto de Geociências e Ciências Exatas, Universidade Estadual Paulista, Campus de Rio Claro, 2016.

MEDEIROS, Fábio. **Criptografia:** Bastão de Licurgo (scytale). 2013. Disponível em: < https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-em-python/>. Acesso em: 10 jul. 2018.

PEREIRA, Nádia Marques Ikeda. **Criptografia:** uma nova proposta de ensino de matemática no ciclo básico. 2015. 78 f. Dissertação (Mestrado em Matemática) – Instituto de Biociências, Letras e Ciências Exatas, Faculdade Júlio de Mesquita Filho, Universidade Estadual Paulista, São José do Rio Preto, 2015.

PORTILHO, Gabriela. **O que é o Manuscrito Voynich?**, 2018. Disponível em: < https://super.abril.com.br/mundo-estranho/o-que-e-o-manuscrito-voynich/>. Acesso em: 08 de out. 2018.

ROQUE, T.; CARVALHO, J. B. P. **Tópicos de História da Matemática.** 1. ed. Rio de Janeiro: SBM, 2012, 467P. (Coleção PROFMAT).

SIERPINSKA, Anna. **On Understanding The Notion Of Function:** The Concept Of Function Aspects Of Epistemology And Pedagogy. 1. ed. Montreal: Concordia University, 1992. 333p.

SILVA, S. L.; SANTOS, R. C.; BRAGANÇA, K. F. **Criptografia:** Uma ferramenta para o estudo de função afim e de sua inversa. 2017. 180 f. Monografia (Licenciatura em Matemática) – Instituto Federal de Educação, Ciência e Tecnologia Fluminense, Campus Campos Centro, Rio de Janeiro, 2017.

SILVA, Ricardo José Aguiar. **Contexto e Aplicações das Funções Exponenciais no Ensino Médio:** Uma Abordagem Interdisciplinar. 2015. 88 f. Dissertação (Mestrado em Matemática) – Centro de Ciências e Tecnologia, Universidade Estadual do Norte Fluminense Darcy Ribeiro, Rio de Janeiro, 2015.

SINGH, Simon. **O livro dos Códigos:** A ciência do sigilo – do antigo Egito à criptografia quântica. 4. ed. Rio de Janeiro: Record, 2004. 448p.

SIQUEIRA, Josué Rangel de. **A Natureza sob um Prisma Matemático.** 2016. 95 f. Monografia (Licenciatura em Matemática) – Instituto Federal de Educação, Ciência e Tecnologia Fluminense, Campus Campos Centro, Rio de Janeiro, 2016.

ZOLNERKEVIC, Igor. **O Código Voynich,** Revista Pesquisa Fapesp, ed. 210 ago. 2013. Disponível em: < http://revistapesquisa.fapesp.br/2013/08/13/o-codigo- voynich/>. Acesso em: 24 de set. 2018.

ANEXO A – Pré-Teste

Atividade para verificar o conhecimento sobre criptografia, função bijetora e a inversa de uma função de estudantes do 9^o ano do Ensino Fundamental II, do Colégio Visão, em Formosa-GO. Esta atividade visa identificar o que os alunos dos anos finais sabem a respeito desses conteúdos. Realização feita pelo discente do Mestrado Profissional em Matemática, Moisés de Oliveira Moura, tendo em vista a elaboração de sua dissertação, orientada pela professora Dr^a. Keidna Cristiane Oliveira Souza.

1- Você sabe o que é criptografia?

2- A criptografia está presente em nosso cotidiano. Você conhece ou sabe de algum aparelho onde ela está sendo utilizada?

3- Você sabe dizer para que serve a criptografia?

4- Você sabe o que é uma função bijetora? E uma função inversa, sabe o que é?

5- Qual é a condição para que uma função admita inversa?

ANEXO B – Pós-Teste

Munidos dos conceitos e das definições mencionadas e embasados nas explicações feitas a respeito do tema abordado, é o momento de colocar em prática o que foi compreendido. A seguir, são propostas algumas atividades acerca desse tema, as quais deverão ser respondidas de forma clara e objetiva.

Atividade - 1 Abaixo temos uma pequena mensagem que foi codificada com a cifra de César, no entanto, não há informação sobre o deslocamento utilizado. Você consegue decifrá-la? (Dica: usar a análise de frequência das letras).
QJXZ ZNOV KMZKVMVYJ:

Atividade - 2 Essa atividade é desenvolvida entre dois indivíduos A e B. O indivíduo A, após organizar o quadro abaixo, pré-codificado com o valor numérico de cada letra do alfabeto, faz a codificação de uma mensagem segundo a função $c(x) = 2x - 9$ e, em seguida, envia para o indivíduo B, juntamente com a função e o quadro. De acordo com as informações, responda as questões a seguir:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

a) Para codificar a mensagem, “A” usou a função $c(x) = 2x - 9$. Para decifrar, “B” terá que usar a função $d(x)$, que é a função inversa de $c(x)$. Qual é a função decodificadora $d(x)$?

b) Ao receber a mensagem codificada, o indivíduo B rapidamente procurou decifrá-la. O que dizia a mensagem?

Mensagem recebida: **4519493945371145 25392919**.

c) O indivíduo B, responde logo após decifrar a mensagem: **“REGRESSO À NOITE”**. Porém, para enviar a mensagem, ele deverá codificá-la. Qual a codificação que “B” deverá enviar para o indivíduo “A”?

d) “B”, só foi capaz de ler a mensagem enviada por “A”, após decifrá-la. Todavia, isso só foi possível porque existe $d(x)$. Como você explicaria a condição da existência de $d(x)$?

ANEXO C – Atividade Final

A ideia essencial no desenvolvimento desse trabalho é estabelecer uma relação entre uma situação recorrente aos alunos com os conteúdos matemáticos trabalhados em sala de aula, além de contemplá-lo com a novidade do tema. Nessa perspectiva, a criptografia foi inserida como instrumento motivador, para enriquecer o ensino de funções afins no 9º ano do Ensino Fundamental. Com base no que está sendo proposto, responda as perguntas a seguir.

1- Você considera a criptografia um tema importante para ser abordado no 9º ano do Ensino Fundamental?

( ) Sim

( ) Não

2- Você achou interessante a ideia central do trabalho, ou seja, inserir a criptografia em conteúdos regulares para torná-los mais interessantes?

( ) Sim

( ) Não

3- O conteúdo de funções afins faz parte da grade curricular do 9º ano do Ensino Fundamental, porém aplicá-lo concomitante com a criptografia é uma proposta do trabalho. No seu entendimento, isso poderá ajudar na compreensão dos conteudos estudados?

( ) Sim

( ) Não

4- O que você diz a respeito da ligação feita entre criptografia e funções?

( ) Não gostei, acho que cada conteúdo deve ser visto separadamente.

( ) Achei muito bom, a ligação entre os dois conteúdos foi perfeita.

5- Dentro da temática do trabalho, o conceito de função inversa foi relevante?

( ) Sim

( ) Não

6- Para fazer a decodificação da mensagem, foi necessário aplicar a inversa de uma função. No entanto, isso só foi possível por causa da bijeção. Para você, a seção função bijetora foi bem colocada no trabalho?

( ) Sim

( ) Não

7- Como você define a ideia do trabalho de um modo geral?

( ) É criativa e pode mudar positivamente o andamento das aulas.

( ) Não causa interesse, portanto, desnecessária sua abordagem.

8- Quanto à introdução dos conceitos de funções bijetora e inversa, marque a opção que melhor condiz com sua opinião.

( ) Desnecessário, pois só aumenta a quantidade de matéria para estudar.

( ) Excelente, pois nos dá uma noção importante para a série seguinte.

9- Em relação à questão anterior, foi difícil compreender a essência desses conteúdos quando tratados com a criptografia?

( ) Sim

( ) Não

10- O que você achou dessa pesquisa?

( ) Não gostei, não vai mudar nada em minha vida

( ) Excelente, pois aprendi o quanto a criptografia é importante e como ela está presente em nossas vidas, além disso, foi muito bom entendê-la juntamente com a matéria estudada em sala de aula.

( ) Gostaria de aprender mais sobre o tema e que fosse visto em mais conteúdos.

( ) É interessante, porém vai aumentar mais ainda os conteúdos para estudar.

( ) Seria bom aprender somente no Ensino Médio.

ANEXO A – Pré-Teste

Atividade para verificar o conhecimento sobre criptografia, função bijetora e a inversa de uma função de estudantes do 9^o ano do Ensino Fundamental II, do Colégio Visão, em Formosa-GO. Esta atividade visa identificar o que os alunos dos anos finais sabem a respeito desses conteúdos. Realização feita pelo discente do Mestrado Profissional em Matemática, Moisés de Oliveira Moura, tendo em vista a elaboração de sua dissertação, orientada pela professora Dr^a. Keidna Cristiane Oliveira Souza.

1- Você sabe o que é criptografia?
É a proteção de um aplicativo celular, sendo um sistema de segurança.

2- A criptografia está presente em nosso cotidiano. Você conhece ou sabe de algum aparelho onde ela está sendo utilizada?
Sim, no Whatsapp.

3- Você sabe dizer para que serve a criptografia?
Para proteger um servidor.

4- Você sabe o que é uma função bijetora? E uma função inversa, sabe o que é?
Não tenho conhecimento sobre o assunto.

5- Qual é a condição para que uma função admita inversa?
Não tenho conhecimento sobre o assunto.

ANEXO A – Pré-Teste

Atividade para verificar o conhecimento sobre criptografia, função bijetora e a inversa de uma função de estudantes do 9^o ano do Ensino Fundamental II, do Colégio Visão, em Formosa-GO. Esta atividade visa identificar o que os alunos dos anos finais sabem a respeito desses conteúdos. Realização feita pelo discente do Mestrado Profissional em Matemática, Moisés de Oliveira Moura, tendo em vista a elaboração de sua dissertação, orientada pela professora Dr^a. Keidna Cristiane Oliveira Souza.

1- Você sabe o que é criptografia?

Não sei, mas imagino que tem a ver com a comunicação e segurança.

2- A criptografia está presente em nosso cotidiano. Você conhece ou sabe de algum aparelho onde ela está sendo utilizada?

Sim, computadores e celulares.

3- Você sabe dizer para que serve a criptografia?

Para fazer sistemas de segurança.

4- Você sabe o que é uma função bijetora? E uma função inversa, sabe o que é?

Não, não.

5- Qual é a condição para que uma função admita inversa?

Não sei.

ANEXO A – Pré-Teste

Atividade para verificar o conhecimento sobre criptografia, função bijetora e a inversa de uma função de estudantes do 9^o ano do Ensino Fundamental II, do Colégio Visão, em Formosa-GO. Esta atividade visa identificar o que os alunos dos anos finais sabem a respeito desses conteúdos. Realização feita pelo discente do Mestrado Profissional em Matemática, Moisés de Oliveira Moura, tendo em vista a elaboração de sua dissertação, orientada pela professora Dr^a. Keidna Cristiane Oliveira Souza.

1- Você sabe o que é criptografia?
Uma forma de esconder mensagens ou dados por meio de alguma "chave", tipo código morse ou binário.

2- A criptografia está presente em nosso cotidiano. Você conhece ou sabe de algum aparelho onde ela está sendo utilizada?
No nosso próprio celular, no aplicativo Whatsapp, as mensagens são criptografadas.

3- Você sabe dizer para que serve a criptografia?
É muito utilizado para compartilhar mensagens secretas ou, no caso do código morse, transmitir mensagens a distância.

4- Você sabe o que é uma função bijetora? E uma função inversa, sabe o que é?
Não sei, mas já ouvi falar.

5- Qual é a condição para que uma função admita inversa?
Não sei.

ANEXO A – Pré-Teste

Atividade para verificar o conhecimento sobre criptografia, função bijetora e a inversa de uma função de estudantes do 9^o ano do Ensino Fundamental II, do Colégio Visão, em Formosa-GO. Esta atividade visa identificar o que os alunos dos anos finais sabem a respeito desses conteúdos. Realização feita pelo discente do Mestrado Profissional em Matemática, Moisés de Oliveira Moura, tendo em vista a elaboração de sua dissertação, orientada pela professora Dr^a. Keidna Cristiane Oliveira Souza.

1- Você sabe o que é criptografia?
É o estudo e a prática de técnicas de comunicação segura na presença de outros.

2- A criptografia está presente em nosso cotidiano. Você conhece ou sabe de algum aparelho onde ela está sendo utilizada?
Sim, ela está presente em nossos smartphones e aplicativos de mensagens, i comunicação.

3- Você sabe dizer para que serve a criptografia?
Para tornar tal comunicação mais segura.

4- Você sabe o que é uma função bijetora? E uma função inversa, sabe o que é?
É um tipo de função matemática que relaciona dois termos. Não sei o que é a Inversa.

5- Qual é a condição para que uma função admita inversa?
Não sei.

ANEXO B – Pós-Teste

Munidos dos conceitos e das definições mencionadas e embasados nas explicações feitas a respeito do tema abordado, é o momento de colocar em prática o que foi compreendido. A seguir, são propostas algumas atividades acerca desse tema, as quais deverão ser respondidas de forma clara e objetiva.

Atividade - 1 Abaixo temos uma pequena mensagem que foi codificada com a cifra de César, no entanto, não há informação sobre o deslocamento utilizado. Você consegue decifrá-la? (Dica: usar a análise de frequência das letras).

QJXZ ZNOV KMZKVMVYJ:

a=V b=W c=X d=Y e=Z f=A g=B h=C i=D

j=E k=F l=G m=H n=I o=J p=K q=L r=M

s=N t=O u=P v=Q w=R x=S y=T z=U

Você está preparado

Cas letras de maior frequência a, e, o

Atividade - 2 Essa atividade é desenvolvida entre dois indivíduos A e B. O indivíduo A, após organizar o quadro abaixo, pré-codificado com o valor numérico de cada letra do alfabeto, faz a codificação de uma mensagem segundo a função $c(x) = 2x - 9$ e, em seguida, envia para o indivíduo B, juntamente com a função e o quadro. De acordo com as informações, responda as questões a seguir:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

a) Para codificar a mensagem, "A" usou a função $c(x) = 2x - 9$. Para decifrar, "B" terá que usar a função $d(x)$, que é a função inversa de $c(x)$. Qual é a função decodificadora $d(x)$?

$c(x) = 2x - 9 \rightarrow d(x) = \frac{x+9}{2}$

b) Ao receber a mensagem codificada, o indivíduo B rapidamente procurou decifrá-la. O que dizia a mensagem?

Mensagem recebida: **4519493945371145 25392919**.

$d(45) = 27$, $d(19) = 14$, $d(49) = 29$, $d(39) = 24$, $d(45) = 27$
$d(37) = 23$, $d(11) = 10$, $d(45) = 27$, $d(25) = 17$, $d(39) = 24$, $d(29) = 19$
$d(19) = 14$
Retornar hoje.

c) O indivíduo B, responde logo após decifrar a mensagem: **"REGRESSO À NOITE"**. Porém, para enviar a mensagem, ele deverá codificá-la. Qual a codificação que "B" deverá enviar para o indivíduo "A"?

$c(x) = 2x - 9$ $c(27) = 45$, $c(14) = 19$, $c(16) = 23$, $c(21) = 45$
$c(14) = 19$, $c(28) = 47$, $c(28) = 47$, $c(24) = 39$, $c(10) = 11$, $c(23) = 37$
$c(24) = 39$, $c(18) = 27$, $c(29) = 49$, $c(14) = 19$
45192345194747 39 11 37392749 19

d) "B", só foi capaz de ler a mensagem enviada por "A", após decifrá-la. Todavia, isso só foi possível porque existe $d(x)$. Como você explicaria a condição da existência de $d(x)$?

Pois, tem que ser uma função bijetora.

ANEXO B – Pós-Teste

Munidos dos conceitos e das definições mencionadas e embasados nas explicações feitas a respeito do tema abordado, é o momento de colocar em prática o que foi compreendido. A seguir, são propostas algumas atividades acerca desse tema, as quais deverão ser respondidas de forma clara e objetiva.

Atividade - 1 Abaixo temos uma pequena mensagem que foi codificada com a cifra de César, no entanto, não há informação sobre o deslocamento utilizado. Você consegue decifrá-la? (Dica: usar a análise de frequência das letras).

QJXZ ZNOV KMZKVMVYJ:

a b c d e f g h i j K l m

V W X Y Z A B C D E F G H

n o p q r s t u v w x y z

I J K L M N O P Q R S T U

letras que mais aparecem a, e, o

Atividade - 2 Essa atividade é desenvolvida entre dois indivíduos A e B. O indivíduo A, após organizar o quadro abaixo, pré-codificado com o valor numérico de cada letra do alfabeto, faz a codificação de uma mensagem segundo a função $c(x) = 2x - 9$ e, em seguida, envia para o indivíduo B, juntamente com a função e o quadro. De acordo com as informações, responda as questões a seguir:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

a) Para codificar a mensagem, "A" usou a função $c(x) = 2x - 9$. Para decifrar, "B" terá que usar a função $d(x)$, que é a função inversa de $c(x)$. Qual é a função decodificadora $d(x)$?

$c(x) = 2x - 9$ $\quad y = \frac{x+9}{2}$

$y = 2x - 9$

$x = 2y - 9$ $\quad \boxed{d(x) = \frac{x+9}{2}}$

$x + 9 = 2y$

b) Ao receber a mensagem codificada, o indivíduo B rapidamente procurou decifrá-la. O que dizia a mensagem?

Mensagem recebida: **4519493945371145 25392919**.

$d(45) = \frac{45+9}{2} = \frac{54}{2} = 27$ $\quad d(25) = \frac{25+9}{2} = \frac{34}{2} = 17$

$d(19) = \frac{19+9}{2} = \frac{28}{2} = 14$ $\quad d(29) = \frac{29+9}{2} = \frac{38}{2} = 19$

$d(49) = \frac{49+9}{2} = \frac{58}{2} = 29$ $\quad d(11) = \frac{11+9}{2} = \frac{20}{2} = 10$

$d(39) = \frac{39+9}{2} = \frac{48}{2} = 24$ Retornar hoje.

$d(37) = \frac{37+9}{2} = \frac{46}{2} = 23$

c) O indivíduo B, responde logo após decifrar a mensagem: **"REGRESSO À NOITE"**. Porém, para enviar a mensagem, ele deverá codificá-la. Qual a codificação que "B" deverá enviar para o indivíduo "A"?

$c(R) = 45$ $\quad c(A) = 11$ $\quad c(I) = 18.2 - 9 = 27$

$c(E) = 29$ $\quad c(N) = 37$ $\quad c(T) = 49$

$c(G) = 2.16 - 9 = 32 - 9 = 23$ $\quad 45292345294747391137392749 29$

$c(S) = 2.28 - 9 = 56 - 9 = 47$

$c(O) = 39$

d) "B", só foi capaz de ler a mensagem enviada por "A", após decifrá-la. Todavia, isso só foi possível porque existe $d(x)$. Como você explicaria a condição da existência de $d(x)$?

Só existe função inversa se a função for bijetora.

ANEXO B – Pós-Teste

Munidos dos conceitos e das definições mencionadas e embasados nas explicações feitas a respeito do tema abordado, é o momento de colocar em prática o que foi compreendido. A seguir, são propostas algumas atividades acerca desse tema, as quais deverão ser respondidas de forma clara e objetiva.

Atividade - 1 Abaixo temos uma pequena mensagem que foi codificada com a cifra de César, no entanto, não há informação sobre o deslocamento utilizado. Você consegue decifrá-la? (Dica: usar a análise de frequência das letras).

QJXZ ZNOV KMZKVMVYJ:

"Você está preparado." deslocamento de 21 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 A B C D E F G H I J K L M N O P

v w x y z

Q R S T U

Atividade - 2 Essa atividade é desenvolvida entre dois indivíduos A e B. O indivíduo A, após organizar o quadro abaixo, pré-codificado com o valor numérico de cada letra do alfabeto, faz a codificação de uma mensagem segundo a função $c(x) = 2x - 9$ e, em seguida, envia para o indivíduo B, juntamente com a função e o quadro. De acordo com as informações, responda as questões a seguir:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

a) Para codificar a mensagem, "A" usou a função $c(x) = 2x - 9$. Para decifrar, "B" terá que usar a função $d(x)$, que é a função inversa de $c(x)$. Qual é a função decodificadora $d(x)$?

$d(x) = \frac{x+9}{2}$

$d(x) = 2x - 9$

$x = 2d(x) - 9$

$d(x) = \frac{x+9}{2}$

b) Ao receber a mensagem codificada, o indivíduo B rapidamente procurou decifrá-la. O que dizia a mensagem?

Mensagem recebida: **4519493945371145 25392919**.

Retornar hoje. $\frac{45+9}{2} = 27$ $\frac{19+9}{2} = 14$ $\frac{49+9}{2} = 29$ $\frac{39+9}{2} = 24$

$\frac{37+9}{2} = 23$ $\frac{11+9}{2} = 10$ $\frac{45+9}{2} = 27$ $\frac{25+9}{2} = 17$

$\frac{29+9}{2} = 19$ $\frac{19+9}{2} = 14$ ↓

$\frac{45+9}{2} = 27$

$\frac{39+9}{2} = 24$

c) O indivíduo B, responde logo após decifrar a mensagem: **"REGRESSO À NOITE"**. Porém, para enviar a mensagem, ele deverá codificá-la. Qual a codificação que "B" deverá enviar para o indivíduo "A"?

45 19 23 45 19 47 47 39 11 37 39 27 49 19

$27 \cdot 2 - 9 = 45$ $14 \cdot 2 - 9 = 19$ $16 \cdot 2 - 9 = 23$ $27 \cdot 2 - 9 = 45$ $14 \cdot 2 - 9 = 10$

$28 \cdot 2 - 9 = 47$ $28 \cdot 2 - 9 = 47$ $24 \cdot 2 - 9 = 39$ $10 \cdot 2 - 9 = 11$ $23 \cdot 2 - 9 = 37$

$24 \cdot 2 - 9 = 39$ $18 \cdot 2 - 9 = 27$ $29 \cdot 2 - 9 = 49$ $14 \cdot 2 - 9 = 19$

d) "B", só foi capaz de ler a mensagem enviada por "A", após decifrá-la. Todavia, isso só foi possível porque existe $d(x)$. Como você explicaria a condição da existência de $d(x)$?

$d(x)$ existe por causa de $c(x)$, já que é a função inversa de $c(x)$.

ANEXO C – Atividade Final

A ideia essencial no desenvolvimento desse trabalho é estabelecer uma relação entre uma situação recorrente aos alunos com os conteúdos matemáticos trabalhados em sala de aula, além de contemplá-lo com a novidade do tema. Nessa perspectiva, a criptografia foi inserida como instrumento motivador, para enriquecer o ensino de funções afins no 9º ano do Ensino Fundamental. Com base no que está sendo proposto, responda as perguntas a seguir.

1- Você considera a criptografia um tema importante para ser abordado no 9º ano do Ensino Fundamental?

- [X] Sim
- [ ] Não

2- Você achou interessante a ideia central do trabalho, ou seja, inserir a criptografia em conteúdos regulares para torná-los mais interessantes?

- [X] Sim
- [ ] Não

3- O conteúdo de funções afins faz parte da grade curricular do 9º ano do Ensino Fundamental, porém aplicá-lo concomitante com a criptografia é uma proposta do trabalho. No seu entendimento, isso poderá ajudar na compreensão dos conteudos estudados?

- [X] Sim
- [ ] Não

4- O que você diz a respeito da ligação feita entre criptografia e funções?

- [ ] Não gostei, acho que cada conteúdo deve ser visto separadamente.
- [X] Achei muito bom, a ligação entre os dois conteúdos foi perfeita.

5- Dentro da temática do trabalho, o conceito de função inversa foi relevante?

(X) Sim

( ) Não

6- Para fazer a decodificação da mensagem, foi necessário aplicar a inversa de uma função. No entanto, isso só foi possível por causa da bijeção. Para você, a seção função bijetora foi bem colocada no trabalho?

(X) Sim

( ) Não

7- Como você define a ideia do trabalho de um modo geral?

(X) É criativa e pode mudar positivamente o andamento das aulas.

( ) Não causa interesse, portanto, desnecessária sua abordagem.

8- Quanto à introdução dos conceitos de funções bijetora e inversa, marque a opção que melhor condiz com sua opinião.

( ) Desnecessário, pois só aumenta a quantidade de matéria para estudar.

(X) Excelente, pois nos dá uma noção importante para a série seguinte.

9- Em relação à questão anterior, foi difícil compreender a essência desses conteúdos quando tratados com a criptografia?

( ) Sim

(X) Não

10- O que você achou dessa pesquisa?

( ) Não gostei, não vai mudar nada em minha vida

(X) Excelente, pois aprendi o quanto a criptografia é importante e como ela está presente em nossas vidas, além disso, foi muito bom entendê-la juntamente com a matéria estudada em sala de aula.

( ) Gostaria de aprender mais sobre o tema e que fosse visto em mais conteúdos.

( ) É interessante, porém vai aumentar mais ainda os conteúdos para estudar.

( ) Seria bom aprender somente no Ensino Médio.

ANEXO C – Atividade Final

A ideia essencial no desenvolvimento desse trabalho é estabelecer uma relação entre uma situação recorrente aos alunos com os conteúdos matemáticos trabalhados em sala de aula, além de contemplá-lo com a novidade do tema. Nessa perspectiva, a criptografia foi inserida como instrumento motivador, para enriquecer o ensino de funções afins no 9º ano do Ensino Fundamental. Com base no que está sendo proposto, responda as perguntas a seguir.

1- Você considera a criptografia um tema importante para ser abordado no 9º ano do Ensino Fundamental?

(✓) Sim

( ) Não

2- Você achou interessante a ideia central do trabalho, ou seja, inserir a criptografia em conteúdos regulares para torná-los mais interessantes?

(✓) Sim

( ) Não

3- O conteúdo de funções afins faz parte da grade curricular do 9º ano do Ensino Fundamental, porém aplicá-lo concomitante com a criptografia é uma proposta do trabalho. No seu entendimento, isso poderá ajudar na compreensão dos conteudos estudados?

(✓) Sim

( ) Não

4- O que você diz a respeito da ligação feita entre criptografia e funções?

( ) Não gostei, acho que cada conteúdo deve ser visto separadamente.

(✓) Achei muito bom, a ligação entre os dois conteúdos foi perfeita.

5- Dentro da temática do trabalho, o conceito de função inversa foi relevante?

(X) Sim

( ) Não

6- Para fazer a decodificação da mensagem, foi necessário aplicar a inversa de uma função. No entanto, isso só foi possível por causa da bijeção. Para você, a seção função bijetora foi bem colocada no trabalho?

(X) Sim

( ) Não

7- Como você define a ideia do trabalho de um modo geral?

(X) É criativa e pode mudar positivamente o andamento das aulas.

( ) Não causa interesse, portanto, desnecessária sua abordagem.

8- Quanto à introdução dos conceitos de funções bijetora e inversa, marque a opção que melhor condiz com sua opinião.

( ) Desnecessário, pois só aumenta a quantidade de matéria para estudar.

(X) Excelente, pois nos dá uma noção importante para a série seguinte.

9- Em relação à questão anterior, foi difícil compreender a essência desses conteúdos quando tratados com a criptografia?

( ) Sim

(X) Não

10- O que você achou dessa pesquisa?

( ) Não gostei, não vai mudar nada em minha vida

(X) Excelente, pois aprendi o quanto a criptografia é importante e como ela está presente em nossas vidas, além disso, foi muito bom entendê-la juntamente com a matéria estudada em sala de aula.

( ) Gostaria de aprender mais sobre o tema e que fosse visto em mais conteúdos.

( ) É interessante, porém vai aumentar mais ainda os conteúdos para estudar.

( ) Seria bom aprender somente no Ensino Médio.

ANEXO C – Atividade Final

A ideia essencial no desenvolvimento desse trabalho é estabelecer uma relação entre uma situação recorrente aos alunos com os conteúdos matemáticos trabalhados em sala de aula, além de contemplá-lo com a novidade do tema. Nessa perspectiva, a criptografia foi inserida como instrumento motivador, para enriquecer o ensino de funções afins no 9º ano do Ensino Fundamental. Com base no que está sendo proposto, responda as perguntas a seguir.

1- Você considera a criptografia um tema importante para ser abordado no 9º ano do Ensino Fundamental?

(●) Sim

( ) Não

2- Você achou interessante a ideia central do trabalho, ou seja, inserir a criptografia em conteúdos regulares para torná-los mais interessantes?

(●) Sim

( ) Não

3- O conteúdo de funções afins faz parte da grade curricular do 9º ano do Ensino Fundamental, porém aplicá-lo concomitante com a criptografia é uma proposta do trabalho. No seu entendimento, isso poderá ajudar na compreensão dos conteudos estudados?

(●) Sim

( ) Não

4- O que você diz a respeito da ligação feita entre criptografia e funções?

( ) Não gostei, acho que cada conteúdo deve ser visto separadamente.

(●) Achei muito bom, a ligação entre os dois conteúdos foi perfeita.

5- Dentro da temática do trabalho, o conceito de função inversa foi relevante?

(x) Sim

( ) Não

6- Para fazer a decodificação da mensagem, foi necessário aplicar a inversa de uma função. No entanto, isso só foi possível por causa da bijeção. Para você, a seção função bijetora foi bem colocada no trabalho?

(x) Sim

( ) Não

7- Como você define a ideia do trabalho de um modo geral?

(x) É criativa e pode mudar positivamente o andamento das aulas.

( ) Não causa interesse, portanto, desnecessária sua abordagem.

8- Quanto à introdução dos conceitos de funções bijetora e inversa, marque a opção que melhor condiz com sua opinião.

( ) Desnecessário, pois só aumenta a quantidade de matéria para estudar.

(x) Excelente, pois nos dá uma noção importante para a série seguinte.

9- Em relação à questão anterior, foi difícil compreender a essência desses conteúdos quando tratados com a criptografia?

(x) Sim

( ) Não

10- O que você achou dessa pesquisa?

( ) Não gostei, não vai mudar nada em minha vida

( ) Excelente, pois aprendi o quanto a criptografia é importante e como ela está presente em nossas vidas, além disso, foi muito bom entendê-la juntamente com a matéria estudada em sala de aula.

(x) Gostaria de aprender mais sobre o tema e que fosse visto em mais conteúdos.

( ) É interessante, porém vai aumentar mais ainda os conteúdos para estudar.

( ) Seria bom aprender somente no Ensino Médio.

ANEXO C – Atividade Final

A ideia essencial no desenvolvimento desse trabalho é estabelecer uma relação entre uma situação recorrente aos alunos com os conteúdos matemáticos trabalhados em sala de aula, além de contemplá-lo com a novidade do tema. Nessa perspectiva, a criptografia foi inserida como instrumento motivador, para enriquecer o ensino de funções afins no 9º ano do Ensino Fundamental. Com base no que está sendo proposto, responda as perguntas a seguir.

1- Você considera a criptografia um tema importante para ser abordado no 9º ano do Ensino Fundamental?

(x) Sim

( ) Não

2- Você achou interessante a ideia central do trabalho, ou seja, inserir a criptografia em conteúdos regulares para torná-los mais interessantes?

(x) Sim

( ) Não

3- O conteúdo de funções afins faz parte da grade curricular do 9º ano do Ensino Fundamental, porém aplicá-lo concomitante com a criptografia é uma proposta do trabalho. No seu entendimento, isso poderá ajudar na compreensão dos conteudos estudados?

(x) Sim

( ) Não

4- O que você diz a respeito da ligação feita entre criptografia e funções?

( ) Não gostei, acho que cada conteúdo deve ser visto separadamente.

(x) Achei muito bom, a ligação entre os dois conteúdos foi perfeita.

5- Dentro da temática do trabalho, o conceito de função inversa foi relevante?

(X) Sim

( ) Não

6- Para fazer a decodificação da mensagem, foi necessário aplicar a inversa de uma função. No entanto, isso só foi possível por causa da bijeção. Para você, a seção função bijetora foi bem colocada no trabalho?

(X) Sim

( ) Não

7- Como você define a ideia do trabalho de um modo geral?

(X) É criativa e pode mudar positivamente o andamento das aulas.

( ) Não causa interesse, portanto, desnecessária sua abordagem.

8- Quanto à introdução dos conceitos de funções bijetora e inversa, marque a opção que melhor condiz com sua opinião.

( ) Desnecessário, pois só aumenta a quantidade de matéria para estudar.

(X) Excelente, pois nos dá uma noção importante para a série seguinte.

9- Em relação à questão anterior, foi difícil compreender a essência desses conteúdos quando tratados com a criptografia?

(X) Sim

( ) Não

10- O que você achou dessa pesquisa?

( ) Não gostei, não vai mudar nada em minha vida

( ) Excelente, pois aprendi o quanto a criptografia é importante e como ela está presente em nossas vidas, além disso, foi muito bom entendê-la juntamente com a matéria estudada em sala de aula.

( ) Gostaria de aprender mais sobre o tema e que fosse visto em mais conteúdos.

( ) É interessante, porém vai aumentar mais ainda os conteúdos para estudar.

(X) Seria bom aprender somente no Ensino Médio.