Universidade Estadual de Londrina

WALMIR PEREIRA SALMAZZO

UMA PROPOSTA DE ATIVIDADES PARA EDUCAÇÃO BÁSICA ENVOLVENDO CRIPTOGRAFIA E FUNÇÕES

Londrina
2021

WALMIR PEREIRA SALMAZZO

UMA PROPOSTA DE ATIVIDADES PARA EDUCAÇÃO BÁSICA ENVOLVENDO CRIPTOGRAFIA E FUNÇÕES

Dissertação apresentada ao Departamento de Matemática da Universidade Estadual de Londrina, como requisito parcial à obtenção do Título de Mestre em Matemática, por meio do PROFMAT – Mestrado Profissional em Matemática em Rede Nacional.

Orientadora: Profª. Dra. Magna Natalia Marin Pires

Londrina
2021

Catalogação elaborada pela Divisão de Processos Técnicos da Biblioteca Central da Universidade Estadual de Londrina

Dados Internacionais de Catalogação-na-Publicação (CIP)

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

S171 SALMAZZO, WALMIR PEREIRA .
UMA PROPOSTA DE ATIVIDADES PARA EDUCAÇÃO BÁSICA ENVOLVENDO CRIPTOGRAFIA E FUNÇÕES / WALMIR PEREIRA SALMAZZO. - Londrina, 2021.
68 f. : il.

Orientador: MAGNA NATALIA MARIN PIRES.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática em Rede Nacional, 2021.
Inclui bibliografia.

1. Matemática na Educação Básica - Tese. 2. Ensino de Matemática - Tese. 3. Criptografia - Tese. 4. Funções - Tese. I. PIRES, MAGNA NATALIA MARIN. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemática em Rede Nacional. III. Título.

CDU 51

WALMIR PEREIRA SALMAZZO

UMA PROPOSTA DE ATIVIDADES PARA EDUCAÇÃO BÁSICA ENVOLVENDO CRIPTOGRAFIA E FUNÇÕES

Dissertação apresentada ao Departamento de Matemática da Universidade Estadual de Londrina, como requisito parcial à obtenção do Título de Mestre em Matemática, por meio do PROFMAT – Mestrado Profissional em Matemática em Rede Nacional.

BANCA EXAMINADORA

_____

Orientadora: Profa. Dra. Magna Natalia Marin Pires
Universidade Estadual de Londrina – UEL

_____

Profa. Dra. Loreni Aparecida Ferreira Baldini
Universidade Estadual do Paraná – UNESPAR

_____

Profa. Dra. Pamela Emanueli Alves Ferreira
Universidade Estadual de Londrina – UEL

Londrina, 16 de abril de 2021.

Dedico a conclusão deste trabalho à minha esposa Rosangela e ao meu filho Lucas, pela força e o incentivo que me deram e por acreditar no meu potencial.

AGRADECIMENTOS

Primeiramente aquele que nos deu o dom da vida, por ter me dado condições, saúde e perseverança para vencer obstáculos, tornando possível cursar e concluir mais este objetivo.

A minha família pela cooperação, incentivo, compreensão e suporte nas etapas difíceis vivenciadas durante toda esta trajetória.

A minha orientadora professora Drª. Magna Natalia Marin Pires, pelo direcionamento brilhante, pela sua disponibilidade, pela paciência inabalável com minhas limitações durante nossas reuniões online, também quero agradecer a professora Drª. Ana Lúcia da Silva, pela organização e participação no desenvolvimento da aplicação da atividade.

Agradeço em especial a Profª. Drª. Loreni Aparecida Ferreira Baldini e a Profª. Drª. Pamela Emanueli Alves Ferreira, que gentilmente aceitaram compor a banca para avaliação do meu trabalho.

Aos colegas de curso e em particular aos bons amigos Carlos e Wander por me acolher e pela parceria criada nas infindáveis horas de sábados dedicadas aos estudos.

Minha gratidão também a todo corpo docente do curso do PROFMAT da Universidade Estadual de Londrina pelo esforço e exemplo de dedicação.

“Não se deve ir atrás de objetivos fáceis,
é preciso buscar o que só pode ser alcançado
por meio dos maiores esforços.”

Albert Einstein

SALMAZZO, Walmir Pereira. **Uma Proposta de Atividades para Educação Básica envolvendo Criptografia e Funções**. 2021. 68 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Estadual de Londrina, Londrina, 2021.

RESUMO

Neste trabalho tem-se como objetivo apresentar uma proposta para o ensino de Matemática no que diz respeito ao conteúdo de Funções na Educação Básica associado à criptografia. Este trabalho apresenta o conceito de criptografia inserida em situações como transmissões de dados, mensagens de aplicativos, informações empresariais, o que garante a segurança e o sigilo dessas informações. O trabalho aborda também a utilização desse conceito durante a História da humanidade. Com este elo a criptografia se apresenta como um conceito motivador e um instrumento de contextualização, fazendo uma relação entre o conteúdo a ser ensinado e situações do cotidiano, em aplicações da Matemática. No desenvolvimento deste trabalho foram apresentados formalmente os conceitos matemáticos, com o objetivo de associá-los ao desenrolar da proposta. O relato do desenvolvimento da primeira atividade com os alunos permitiu inferir que trabalhos como este promovem o envolvimento e a aprendizagem dos estudantes no que diz respeito aos conceitos de domínio, imagem, função inversa, imagem inversa dentre outros.

Palavras-chave: ensino de matemática; criptografia; funções; educação básica.

SALMAZZO, Walmir Pereira. **A Proposal for Activities for Basic Education involving Cryptography and Functions**. 2021. 68 p. Dissertation (Professional Master in Mathematics in National Network) - State University of Londrina, Londrina, 2021.

ABSTRACT

This work aims to present a proposal for the teaching of Mathematics with regard to the content of Functions in Basic Education associated with cryptography. This paper presents the concept of encryption inserted in situations such as data transmissions, application messages, business information, which guarantees the security and confidentiality of this information. The work also addresses the use of this concept during the history of humanity. With this link, cryptography presents itself as a tool, a motivating concept and an instrument of contextualization, making a connection between the content to be taught and a daily situation, in applications of Mathematics. In the development of this work, the mathematical concepts were formally presented, with the objective of associating them to the development of the proposal. The report of the development of the first activity with the students made it possible to infer that works like this promote the students' involvement and learning with regard to the concepts of domain, image, inverse function, inverse image among others.

Keywords: mathematics teaching; cryptography; functions; basic education.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

Como professor de matemática por mais de 20 anos, sempre busco contextualizar os conteúdos, aprender novas formas de conduzir a aula, na tentativa de dar sentido ao que se ensina e tornar as aulas mais interessantes. D'Ambrósio (1998, apud Ferreira, 2015, p. 3) defende que, a matemática

> está passando por profundas transformações. O professor, necessariamente, deve estar mais preparado para participar dessas transformações e para se aventurar no novo, do que para repetir o velho, muitas vezes inútil e desinteressante. [...] Hoje se espera criatividade e não basta repetir aquilo que foi ensinado. [..] O novo perfil do professor é fundamentalmente o de um facilitador da aprendizagem do aluno e de um companheiro na busca do novo.

Em busca de uma educação de qualidade, novas práticas de ensino vêm avançando no campo do ensino de Matemática. Uma sociedade justa com cidadãos bem formados só se faz com educação de qualidade.

A educação é um fator de mudança na sociedade, para Pinto e Dias (2019)

> a educação exerce forte influência nas transformações da sociedade. A nosso ver, a educação reforça a capacidade crítica do indivíduo e atesta o grau de desenvolvimento de uma sociedade. Quanto mais desenvolvida ela for, mais facilmente se compreenderá o papel da educação. Também é lícito referir que, em virtude de uma maior capacidade de análise que os seus cidadãos têm, maior será a transmissão do conhecimento, maior o nível do debate e da consciência com os deveres e as responsabilidades na defesa e na promoção dos direitos humanos e sociais (PINTO; DIAS, 2019, p. 450).

Considerando características de uma educação de qualidade, o conhecimento matemático é um importante componente no processo de formação do cidadão, com ele podemos resolver uma infinidade de situações, o qual nos dá suporte para outras áreas do conhecimento. Os Parâmetros Curriculares Nacionais Mais Ensino Médio, corrobora com essa ideia.

> [...] aprender Matemática de uma forma contextualizada, integrada e relacionada a outros conhecimentos traz em si o desenvolvimento de competências e habilidades que são essencialmente formadoras, à medida que instrumentalizam e estruturam o pensamento do aluno, capacitando-o para compreender e interpretar situações, para se apropriar de linguagens específicas, argumentar, analisar e avaliar,

> tirar conclusões próprias, tomar decisões, generalizar e para muitas outras ações necessárias à sua formação. (BRASIL, 2002, p. 111).

Para Ferreira (2013) a contextualização da matemática fortalece em cada educando uma independência nas tomadas de decisões e também ajuda na estruturação do pensamento e no raciocínio dedutivo. De acordo com PCNEM[1],

> [...] a Matemática contribui para o desenvolvimento de processos de pensamento e a aquisição de atitudes, cuja utilidade e alcance transcendem o âmbito da própria Matemática, podendo formar no aluno a capacidade de resolver problemas genuínos, gerando hábitos de investigação, proporcionando confiança e desprendimento para analisar e enfrentar situações novas, propiciando a formação de uma visão ampla e científica da realidade, a percepção da beleza e da harmonia, o desenvolvimento da criatividade e de outras capacidades pessoais. (BRASIL, 2000, p. 40).

Inspirados nesta visão de Matemática, de ensino de Matemática e, considerando que uma das exigências do PROFMAT (Programa de Mestrado Profissional em Matemática em Rede Nacional) é que o aluno desenvolva um trabalho de conclusão sobre temas específicos pertinentes ao currículo de Matemática da Educação Básica com impacto na prática didática em sala de aula, desenvolvemos um trabalho abordando o conteúdo de Funções por meio de tarefas que envolvem criptografia.

O objetivo dessa dissertação é apresentar uma proposta para o ensino de Matemática no que diz respeito ao conteúdo de Funções na Educação Básica associado à criptografia. Para alcançar esse objetivo seguimos as seguintes ações:

- apresentar atividades matemáticas que envolvam codificar e decodificar mensagens, para alunos da Educação Básica abordando o conteúdo de funções;
- reconhecer, analisar e discutir conceitos relacionados ao conteúdo de funções a partir dos que os alunos expressam (ou podem expressar) ao lidar com atividades de codificação e decodificação de mensagens;
- apresentar definições matemáticas no contexto da criptografia.

[1] Parâmetros Nacionais do Ensino Médio.

Para isso, foram elaboradas duas atividades que desencadeiam uma discussão do conteúdo de Funções, a primeira foi desenvolvida com alguns alunos de forma remota, realizamos a descrição da aula para analisarmos os entendimentos expressados por eles e sugerimos como o professor poderia utilizar essas observações que os alunos fazem para desenvolver os conteúdos matemáticos. A segunda tarefa é apresentada com observações e hipóteses de como alunos e professores podem abordá-las.

Assim, além dessa introdução, este trabalho está subdividido em quatro capítulos e mais as considerações finais. No primeiro capítulo apresentamos uma fundamentação teórica e um histórico sobre o uso da criptografia pelo homem, uma forma de ajudar a comunicação ou transmissão de informações de maneira sigilosa e segura, como exemplo podemos citar situações de guerras, tanto nas civilizações antigas como nas atuais.

Hoje o uso da criptografia gira em torno da criação de novos e eficientes meios de proteção para a transmissão de dados financeiros (bolsa de valores, instituições financeiras), já para a sociedade em geral, a criptografia está diretamente ligada na comunicação entre pessoas, ou seja, aplicativos de celulares (WhatsApp ou mesmo e-mail). Além de apresentar a relação existente entre a esteganografia, criptografia e a criptoanálise.

No segundo capítulo trazemos as definições matemáticas envolvidas na nossa proposta de trabalho, além de relatar os diferentes conceitos existentes da definição de função e a sua evolução entre os famosos matemáticos como Bernoulli, Euler, Fourier, Dirichlet e Riemann.

No terceiro capítulo apresentamos os procedimentos metodológicos para o desenvolvimento desse trabalho, as atividades elaboradas para a realização desse estudo no formato de uma proposta para sala de aula. No quarto capítulo temos a descrição da aplicação da primeira tarefa.

Para finalizar, apresentamos nossas considerações a respeito da realização do trabalho do ponto de vista da formação do autor e também da colaboração desse trabalho para professores da Educação Básica.

CAPÍTULO 1
FUNDAMENTAÇÃO TEÓRICA

1.1 CRIPTOGRAFIA

A comunicação entre pessoas é algo surpreendente, pois temos várias maneiras de nos comunicarmos, por fala, por escrita, por sinais, pelo olhar. Porém, em determinadas situações a comunicação deve ser discreta ou mesmo disfarçada, dentre muitos exemplos podemos citar a interação entre parceiros em um jogo de cartas, o envio de uma mensagem em que só o receptor possa conhecê-la. Para resolver esses tipos de questões o homem criou códigos ou símbolos para serem interpretados apenas por aqueles a quem a mensagem se destina.

Hoje em dia, no nosso cotidiano, informações de segurança devem ser mantidas em secreto, uma compra online, uma transação financeira, uma conversa entre confidentes, entre outros exemplos. Tanto no campo pessoal como no financeiro, o sigilo é muito importante em um negócio, isto tudo devido à automação de processos que usa os dispositivos computacionais conectados à rede. No entanto, este benefício e praticidade trazida pela automação tecnológica não vem sozinha, pois há riscos gerados pela movimentação de dados confidenciais na rede mundiais, o que traz a preocupação com a segurança, a qual leva à criação de criados recursos tecnológicos para proteger dados e informações dessas ameaças.

A Criptografia é a ciência que estuda a escrita cifrada reunindo técnica e conhecimentos para o armazenamento de informações e dados de maneira segura e sigilosa (codificada). De acordo com Alves (2017), temos que a

> criptografia pode ser entendida como um conjunto de técnicas e métodos que, por meio de uma chave ou conjunto de chaves, tem por fim de mascarar uma informação, denominada texto aberto ou **textitcleartext** convertendo está em uma informação incompreensível denominada texto cifrado ou /**textitcyphertext** de maneira que somente quem saiba o segredo por trás de método consiga reverter o texto cifrado em texto claro (ALVES, 2017, p. 16, negrito nosso).

Para Kahn (1973, apud Moura, 2019), criptografia 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 apud MOURA, 2019 p. 15).

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

A codificação feita pela criptografia está ligada ao sigilo das informações e a decifragem ou a criptoanálise é a ação de quebra dos dados codificados.

Podemos dizer ainda que a criptoanálise é a arte de tentar descobrir o texto cifrado e/ou a lógica utilizada em sua encriptação (chave), ela representa o empenho de decodificar ou decifrar mensagens sem que se tenha o conhecimento prévio da chave secreta que as gerou. As diversas técnicas de criptoanálise são os caminhos que os analistas podem seguir para conseguir descobrir ou quebrar a codificação das mensagens que estiverem cifradas, e não apenas a simples decifração de uma mensagem.

> (...) além de empregar cifras, os estudiosos árabes foram capazes de quebrá-las. Eles inventaram a criptoanálise, a ciência que permite decifrar uma mensagem sem conhecer a chave. Enquanto o criptógrafo desenvolve métodos de escrita secreta, é o criptoanalista que luta para encontrar fraquezas nesses métodos, de modo a quebrar a mensagem secreta. Os criptoanalistas árabes tiveram sucesso na descoberta de um método para quebrar a cifra de substituição monoalfabética, uma cifra que tinha permanecido invulnerável durante vários séculos (SINGH, 2020, p. 32).

É possível codificar uma informação de duas maneiras. Uma delas é conhecida por **esteganografia**.

A esteganografia é a arte de esconder informações. Mais especificamente, um meio é escolhido para que uma informação seja camuflada, de modo a evitar que terceiros possam obtê-la. Evidências de seu uso podem ser encontradas ainda na Grécia Antiga.

Segundo Jascone (2003, p.34),

> a esteganografia é a arte de comunicar-se secretamente, ocultando uma mensagem sigilosa dentro de outra informação sem importância, de maneira que não exista forma de detectar que há uma mensagem escondida. Na computação essa outra informação pode ser um arquivo de som, imagem ou texto.

Para Popa (1998, p.2), “esteganografia deriva do grego, onde estegano = esconder ou mascarar e grafia = escrita”. Assim, esteganografia é a arte da escrita para comunicações ocultadas. Para Petri (2004), dentro da esteganografia

> existe um conjunto de métodos para comunicações secretas desenvolvidas ao longo da história. Como exemplo destes métodos pode destacar: tintas “invisíveis”, micropontos, arranjo de caracteres (character arrangement), assinaturas digitais, canais escondidos (covert channels), comunicações por espalhamento de espectro (spread spectrum communications), entre outras (PETRI, 2004, p.7).

Para exemplificar uma aplicação atual da esteganografia digital podemos citar a “marca d’água”, mensagem oculta dos direitos autorais, e a “impressão digital”, número de série ou conjunto de caracteres que autêntica uma cópia legítima. A falta da “impressão digital” aponta violação de direito autoral e a ausência da “marca d’água” comprova o fato (DANTAS, 2002).

Além da esteganografia, temos também a criptografia que utiliza técnicas para esconder o sentido da mensagem, ou seja, técnicas para codificar ou mesmo cifrar a escrita tornando-a ininteligível para aqueles que não tenham acesso as convenções combinadas ou as chaves de codificação.

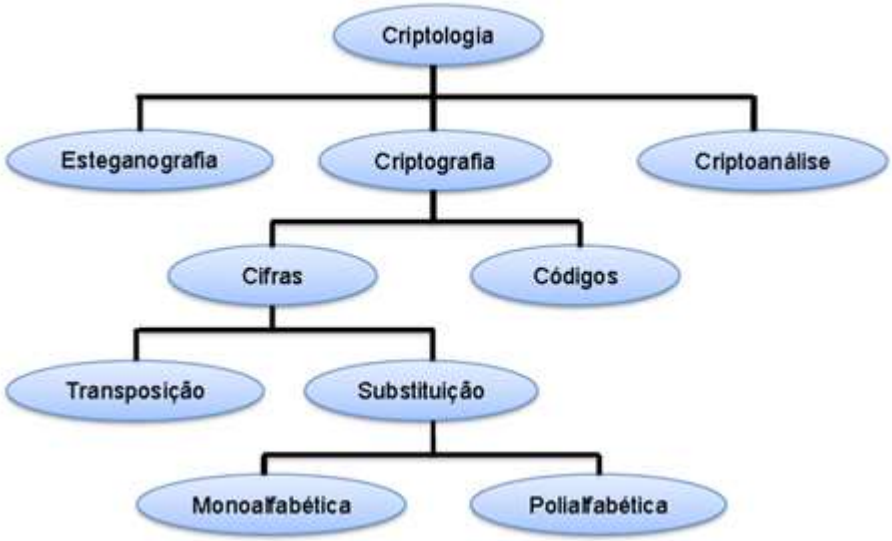
Chaves de codificação ou chaves de encriptação é um conjunto de caracteres que no processo de encriptação é utilizado para "bagunçar"/codificar, mascarar os dados ou as informações confidenciais de forma a que estes fiquem encriptados, quanto mais randômica/imprevisível esta chave for, mais difícil será que alguém externo ao processo consiga desencriptar a informação. Por exemplo, no caso da criptografia RSA[2], utiliza-se de duas chaves, citada por Filho e Malagutti (2013):

> A ideia do sistema é a seguinte: uma das chaves serve para cifrar mensagens e pode ser divulgada livremente – todos têm acesso a ela – por isso é conhecida como *chave pública*. Por outro lado, para decifrar a mensagem cifrada, há a necessidade de uma chave secreta, conhecida apenas pela pessoa para a qual a mensagem foi enviada, por isto essa chave é conhecida como *chave secreta*. (FILHO; MALAGUTTI, 2013, p. 73).

A figura a seguir mostra um esquema de Bezerra, Malagutti e Rodrigues (2010), a estrutura da criptologia e suas ramificações.

[2] O acrônimo RSA é o algoritmo de chave pública mais utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecida. O nome RSA é composto das letras iniciais dos sobrenomes de Ron Rivest, Adi Shamir e Leonard Adleman, fundadores da atual empresa RSA Data Security, Inc. (SANTOS, 2013).

Figura 1 – Diagrama da Criptografia e suas ramificações



Fonte: Bezerra; Malagutti e Rodrigues (2010)

A partir de algumas reflexões e, considerando as definições dos autores, podemos dizer que a criptografia é a arte ou a ciência de escrever mensagens ou informações confidenciais em cifra ou em código, ou seja, ela é constituída por um conjunto de técnicas que propicia tornar inteligível uma informação originalmente escrita com uma boa percepção, de maneira que somente o destinatário a decodifique e a compreenda.

Nos dias atuais, entretanto, com a expansão da tecnologia e consequentemente a comunicação eletrônica, a criptografia deixou de ser apenas um meio de esconder mensagens, pois a dependência da rapidez e da transmissão de dados, principalmente aquelas que abrange transações financeiras e uso seguro da internet, evidenciou cada vez mais sua importância e desenvolvimento.

No início a criptografia era vista como uma arte, atualmente passou a ser conceituada como uma ciência. Algumas aplicações da criptografia atualmente estão ligadas diretamente com:

- ✓ sigilo em banco de dados;
- ✓ censos;
- ✓ investigações governamentais;
- ✓ dossiês de pessoas sob investigação;
- ✓ dados hospitalares;
- ✓ informações de crédito pessoal;

- ✓ decisões estratégicas empresariais;
- ✓ sigilo em comunicação de dados;
- ✓ comandos militares;
- ✓ mensagens diplomáticas;
- ✓ operações bancárias;
- ✓ comércio eletrônico;
- ✓ transações por troca de documentos eletrônicos (EDI);
- ✓ estudo de idiomas desconhecidos;
- ✓ recuperação de documentos arqueológicos, hieróglifos;
- ✓ e até tentativas de comunicações extraterrestres!

A criptografia é algo intrigante, pois pode proporcionar situações que envolvem várias emoções, algo como um desafio. Os desafios, são considerados pelo ser humano com fascínio, atraindo-os para chegarem as suas soluções. Temos como exemplo toda a história da criptografia da antiguidade, se os arqueólogos não se sentissem desafiados a descobrirem o que estava por detrás dos símbolos, ou dos enigmas que cada artefato possuía, não saberíamos como era o povo, as condições de vida e até mesmo como foram as tomadas de decisões em situações da época que viveram. Podemos utilizar essas ideias nas aulas de matemática, se o educando não se sentir desafiado para resolver ou chegar a solução de um exercício certamente não teremos êxito, a criptografia pode ser uma das ferramentas para aflorar o desafio no educando.

1.2 CRIPTOGRAFIA: ASPECTOS HISTÓRICOS

A criptografia fez e faz parte de vários momentos históricos da humanidade. Desde os tempos mais remotos, com a necessidade da comunicação e com a evolução da escrita, podemos destacar vários acontecimentos na história em que se fez uso da criptografia. Vamos trazer alguns exemplos em que a troca de informações de maneira sigilosa (criptografadas) influenciaram ou tiveram um papel fundamental em decisões que envolviam batalhas em guerras, situações políticas com seus segredos políticos ou descrições em tumbas para aumentar o mistério em torno da sua própria história.

A seguir apresentamos alguns objetos que compõe essa história.

Segundo Machado (2020), registros mostram que os homens das cavernas deviam se comunicar através de gestos, posturas, gritos e grunhidos, assim como os demais animais não dotados da capacidade de expressão mais refinada. Os povos sumérios, umas das civilizações mais antiga do mundo, que ocupava a região da Mesopotâmia, foi a primeira a usar o sistema pictográfico (escritas feitas nas cavernas, com tintas). Outra civilização a utilizar este tipo de escrita foram os egípcios que em 3100 a.C., criaram seus *hierós glyphós* ou “escrita sagrada”.

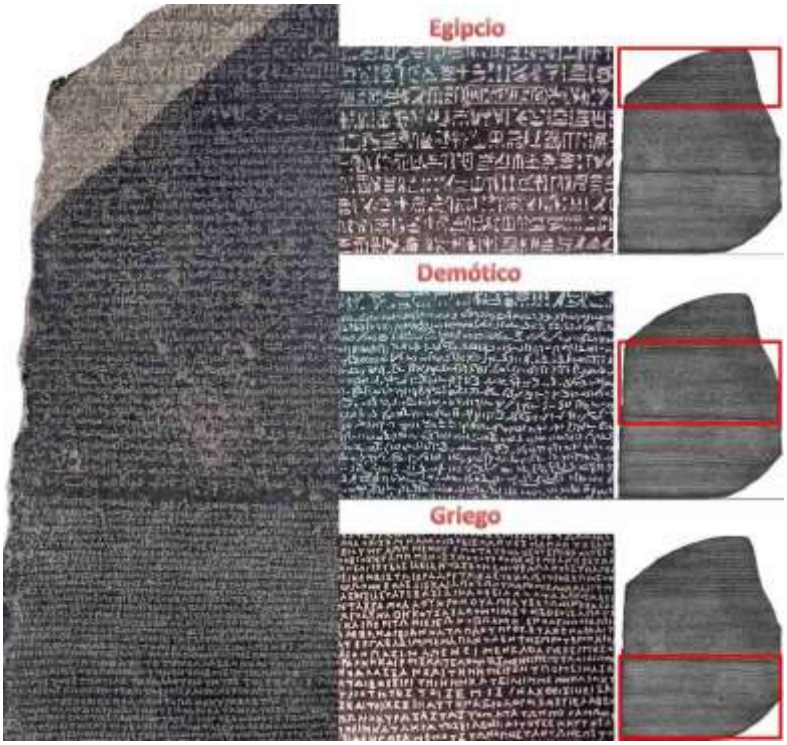
De acordo Singh (2020), com o surgimento da escrita uma grande preocupação foi crescente, privacidade e segurança se tornou algo importantíssimo para proteger e esconder informações ou segredos militares. Temos relatos que em uma vila egípcia, denominada por Menet Khufu, na proximidade do rio Nilo, cerca de 1900 a.C. no túmulo de Khnumhotep II, um importante arquiteto do faraó Amenemhet, foi encontrado uma dessas técnicas, na qual algumas palavras ou trechos eram substituídos por outros.

Temos ainda, uma outra situação similar, a Pedra de Rosetta, que se encontra no British Museum, homenageando o rei Ptolomeu V, é um fragmento de uma estela de granodiorito do Antigo Egito, encontrada próxima à cidade de El-Rashid, após a derrota de Napoleão para o Reino Unido. Nela temos uma técnica de escrita que envolve três tipos de alfabetos: hieróglifo, demótico e grego, além de ter sido escrito em duas línguas.

Figura 2 - Pedra de Roseta, exposta do Museu Britânico, em Londres

(Foto: Flickr/Malcom Manners/Creative Commons)
Fonte: https://letsflyaway.com.br/wp-content/uploads/2015/05/pedra-roseta-museu-britanico.jpeg

Figura 3 - Três tipos de alfabeto



Fonte: https://amigopai.wordpress.com/2015/06/07/hieroglifos-ou-hieroglifos/

O responsável por desvendar esses símbolos foi Jean-Francois Champollion, que concluiu que os sinais empregados exprimiam ideias e alguns sons, ou seja, muitos hieróglifos possuíam um valor de efeito fonético.

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, 2020, 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, 2020, p. 25).

O sistema de criptografia envolvido nesta situação era constituído de um bastão de madeira ao qual era enrolado, ao seu redor, uma fita ou cinto de couro ou pergaminho. Para escrever a mensagem secreta neste cinto, existia todo um procedimento a ser executado, as letras deveriam ser escritas no sentido do comprimento do bastão e, depois, bastaria desenrolar a tira, para obter o conteúdo da mensagem cifrada.

Figura 4 – Bastão de Licurgo

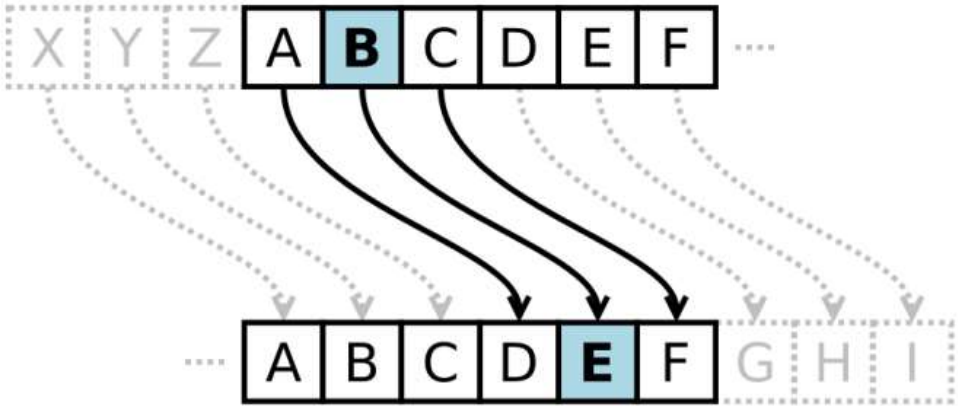
Fonte: Medeiros (2013)

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, 2020, p. 422). O algoritmo da cifra, neste caso, é o enrolar da tira no bastão e a chave, a sua largura.

Segundo Singh (2020), o líder militar e governante romano, Caio Júlio César (100 a.C. – 44 a.C.) desempenhou 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.

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 5, a letra A era substituída pela letra D, a letra B era substituída pela letra E, e assim sucessivamente.

Figura 5 – 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).

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, 2020, p. 26).

De acordo com Moura (2019), se uma codificação usar a cifra de substituição de César, potencialmente poderá decifrar a mensagem 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. Assim, será inviável ao inimigo tentar decifrá-la, já que existem aproximadamente 400.000.000.000.000.000.000.000.000 de chaves diferentes.

Após o surgimento da análise de frequência no mundo árabe, surgiu uma técnica que permite decifrar uma mensagem sem conhecer a chave, percebe-se a vulnerabilidade da cifra de substituição monoalfabética,

> 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 22 ibn Ismail al-Kindi. Conhecido como “o filólosofo dos árabes” (SINGH, 2020, p. 33).

Frente à fragilidade da cifra de substituição monoalfabética, os criptógrafos, “pessoa especializada em desenvolver novos métodos de escrita

secreta” (SINGH, 2020, 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, 2020, 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 alfabética está 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 (2020), 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.

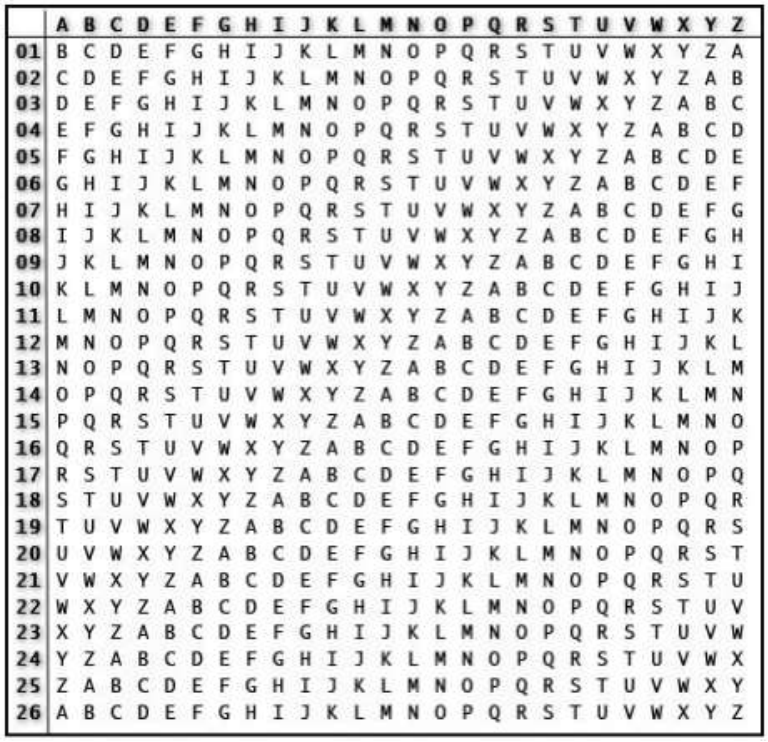
Figura 6 – Blaise de Vigenère

Fonte: Singh (2020)

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 7.

Figura 7 – O quadrado de Vigenère



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	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
02	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
03	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
04	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
05	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
06	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
07	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
08	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
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Singh (2020)

Esses são apenas alguns exemplos da criptografia na história da humanidade. Essas ideias foram evoluindo e hoje sistemas de códigos complexos são utilizados em transações financeiras, transmissões de dados e comunicação entre pessoas.

1.3 A CRIPTOGRAFIA NA ATUALIDADE.

O advento da tecnologia computacional no início dos anos 70, mais especificamente com o aparecimento das grandes redes de comunicação (internet) no mundo, trouxe agilidade e praticidade tanto na comunicação entre pessoas como na interação entre as instituições financeiras, no comércio online tão explorado, principalmente nesta época de epidemia. Para assegurar o sigilo dessas comunicações e transações uma ferramenta é necessária: a criptografia.

A criptografia se tornou algo indispensável nos dias atuais, já que está em muitas coisas que envolve nosso dia a dia, protegendo e dando acessibilidade somente as verdadeiras partes interessadas. A criptografia permite sigilo em dados

bancários, arquivos compartilhados na nuvem, e-mails, reuniões e até a mais simples mensagem no WhatsApp.

Devido ao avanço muito rápido da tecnologia, a criptografia teve também que sofrer atualizações para se adequar a esses avanços. Alguns desses avanços foram os desenvolvimentos dos vários sistemas criptográficos, como exemplo mencionamos a área da computação, que se utiliza de métodos que contêm o conceito de chaves" baseado em conjuntos de *bits* e algoritmos preparados para codificar e decodificar informações ou dados, onde o emissor e o receptor possuem chaves compatíveis. Sem esse conjunto o acesso para extrair o conteúdo fica impossibilitado.

Tivemos durante a história da criptografia métodos que eram conhecidos por Chaves Simétricas e Chaves Assimétricas.

Chaves Simétricas, que para Alecrim (2005, apud VICENTE; ARAÚJO; ROCHA; ALMEIDA E HADDAD, 2016, p.6) é um tipo de chave mais simples, da qual o emissor e o receptor fazem uso dela, isto é, para codificação e descodificação é utilizada a mesma chave.

Figura 8 - Chave Simétrica

Fonte: Vicente; Araújo; Rocha; Almeida e Haddad (2016)

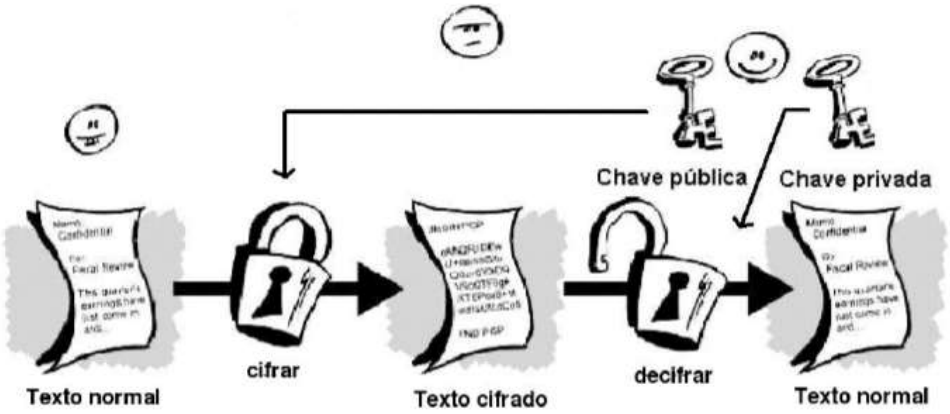
De acordo com Vicente; Araújo; Rocha; Almeida e Haddad (2016), para este tipo de algoritmos de chaves simétricas, nos dias atuais, temos:

- DES (Data Encryption standard) criado em 1977;
- IDEA (International Data Encryption Algorithm) criado em 1991 e
- RC (Ron´s Code ou Rivest Cipher) criado em 1994, muito utilizado por provedores de e-mails tendo versões (RC2, RC4,

RC5 e RC6) que difere uma da outra por trabalhar com chaves maiores.

Segundo Quaresma (2007 apud VICENTE; ARAÚJO; ROCHA; ALMEIDA E HADDAD, 2016, p.7), no sistema de Criptografia Assimétrica ou de chave pública, o processo de cifração usa uma chave pública, porém o processo de decifração usa uma chave diferente, dita chave privada.

Figura 9 - Chave Assimétrica



Fonte: Vicente; Araújo; Rocha; Almeida e Haddad (2016)

Os principais algoritmos que utilizam chaves assimétricas são: RSA (Rivest, Shamir and Adleman): criado em 1977, sendo esse o mais utilizado, outro é o ElGamal criado em 1984, sendo utilizado em assinaturas digitais.

As assinaturas digitais são produtos de outro sistema de segurança que faz uso da criptografia assimétrica, visando certificar a integridade de dados ou documentos amplamente utilizados na atualidade. Essas assinaturas digitais foram criadas devido a expansão da informática e a migração do mercado em geral para o ambiente digital.

A preocupação em tornar segura nossa vida digital, garantindo todo processo e todo procedimento computacional só é possível devido a criptografia. Ao utilizarmos nosso smartphone para realizarmos pagamentos, consulta de saldo, transferências bancárias e outras transações, estamos nos beneficiando da criptografia.

CAPÍTULO 2
FUNÇÃO

2.1 CONCEITO DE FUNÇÃO

Entende-se por função a relação de dependência entre duas grandezas, ou seja, para termos uma função precisamos satisfazer duas condições:

1) estabelecer dois conjuntos, um primeiro conjunto, do qual tomaremos os valores da variável independente, e um segundo, no qual encontraremos os valores correspondentes da variável dependente;
2) haver uma relação entre as duas grandezas em que para cada valor tomando no primeiro conjunto corresponda um único elemento do segundo conjunto.

Podemos também entender uma função da seguinte maneira: quando entre duas grandezas, A e B quaisquer, existe uma correspondência e para cada valor ou medida de A ocorre uma e somente uma única medida correspondente de B, então dizemos que B está em função de A ou que temos uma função de A em B.

Este é um conceito matemático importante e de muito valia e aplicação em nosso cotidiano.

O conceito de função se tornou, na Matemática, um dos mais importantes, pois a partir do século XVII ele vem autenticando e consolidando outros conceitos matemáticos, temos como exemplo os conceitos do Cálculo Diferencial e Integral.

Assim, ao detectarmos regularidades em algum evento, que conceito matemático podemos utilizar? Primeiro que vem à mente é função, pois está presente na maioria das situações do dia a dia, além de ter seu campo próprio para o estudo das leis que regem. Por isso é incontestável sua relevância e aplicabilidade em variadas áreas, dentre outras, as áreas da Física, Química, Ciências Contábeis, Economia, Ciência da Computação.

Para refletimos o conceito de função podemos também nos referirmos a algumas frases do cotidiano como: “uma coisa depende da outra” ou “uma coisa está em função da outra”; levando essa ideia para o campo da Matemática, nas

funções o valor de uma variável depende o valor de outra variável, e essa ideia compõe as variáveis dependente e as independentes. Os gráficos podem nos mostram com simplicidade essa relação entre as variáveis.

Outro detalhe importante está nas evoluções sofridas pelo conceito de função entre os matemáticos durante os anos. Por exemplos: por volta do ano 200 a.C. os babilônicos resolviam equações quadráticas através de métodos que hoje seria o da substituição. E mais, de acordo com Baumgart (1992),

> [...] dever ia-se creditar aos babilônios uma definição operacional de função devido ao uso que faziam com tabelas, como por exemplo $n^3 + n^2$, n = 1, 2, 3, 4,..., 30,..., sugerindo a definição de que uma função é uma tabela ou uma correspondência entre n e $n^3 + n^2$. (BAUMGART, 1992, p. 83).

No século XVII, encontramos a definição de função introduzida por Leibniz associando este conceito às curvas, onde curva e imagem geométrica de uma função se tornaram sinônimos.

Já no século XVIII, Johann Bernoulli e Euler consideraram uma função como uma expressão qualquer associada a uma variável e à constantes. Foi Euler que introduziu a notação *f(x).* Nos meados do século XIX outro matemático contribuiu com a teoria de funções, Joseph Fourier.

Com a criação das bases para as reformulações das ciências ao final do século XVIII, os matemáticos começaram a estabelecer uma fundamentação lógico-rigorosa ao saber existente. Fatos estes que levaram Johann Peter Gustav Lejeune Dirichlet, já no século XIX, a associar a noção de variável a noção de função, como mencionado em (EVES, 2011):

> Uma variável é um símbolo que representa um qualquer dos elementos de um conjunto de números; se duas variáveis x e y estão relacionadas de maneira que, sempre que se atribui um valor a x, corresponde automaticamente, por alguma lei ou regra, um valor a y, então se diz que y é uma função (unívoca) de x. A variável x, à qual se atribuem valores à vontade, é chamada variável independente e a variável y, cujos valores dependem dos valores de x, é chamada variável dependente. Os valores possíveis que x pode assumir constituem o campo de definição da função e os valores assumidos por y constituem o campo de valores da função (EVES, 2011, p. 661).

Para Ramos (2013, p. 3), “essa é a definição mais moderna de função que encontramos nos livros de Matemática que nos apresenta de uma forma mais

ampla a relação entre dois conjuntos numéricos que extrapola e independe da forma analítica de relação entre x e y."

Outra definição de função está ligada diretamente com a Teoria dos Conjuntos de Cantor, que permitiu a Riemann (século XIX) definir uma função f como uma relação dada por um conjunto de pares ordenados que obedecem à seguinte condição: se os pares (x_1, y_1) e (x_2, y_2) pertencem a f, e $x_1 = x_2$, logo $y_1 = y_2$. O conjunto dos primeiros elementos dos pares ordenados é o domínio da função, e o conjunto de todos os segundos elementos dos pares ordenados se diz imagem da função. Assim, uma função é simplesmente um tipo particular de subconjunto do produto cartesiano de dois conjuntos. (EVES, 2011, p. 660-661)

Os estudos de funções obtiveram um grande avanço entre os séculos XVII a XIX, através das contribuições dadas pelos famosos matemáticos como Bernoulli, Euler, Fourier, Dirichletn e Riemann.

2.2 ALGUMAS DEFINIÇÕES LIGADAS A DIERENTES CAMPOS DA MATEMÁTICA

Apresentamos a seguir a definição de função em três diferentes áreas da matemática.

• Definição utilizando a Teoria de Conjuntos de Dirichlet – Riemann, séc. XIX:
Sejam x e y duas variáveis representativas de conjuntos de números; diz-se que y é função de x e escreve-se y = f(x) se entre as duas variáveis existe uma correspondência unívoca no sentido x → y. a x chama-se variável independente, a y variável dependente (CARAÇA, 1989, p. 129).

• Definição analítica de Bernoulli – séc. XVII:
Este modo de definição consiste em dar um conjunto de operações de modo tal que, por meio delas, se possa fazer corresponder a cada valor de x um valor de y. Demos, por exemplo, a igualdade $y = 4{,}9.x^2$ (CARAÇA, 1989, p. 130).

• Definição geométrica de função de Leibniz – séc. XVII:
Seja um sistema cartesiano e uma curva C que não seja cortada em mais de um ponto por uma reta paralela ao eixo Oy. Essa curva permite definir uma função y(x) (CARAÇA, 1989,p. 133).

2.3 DEFINIÇÕES[3]

Dados dois conjuntos *A* e *B*[4], 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 $(x, y) \in f$

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

A é chamado domínio ou campo de definição.

B é chamado contradomínio.

$Im\,(f) = \{y \in B \mid \exists \mid x \in A\}$ com $f(x) = y$ é chamado conjunto imagem de f.

Domínio e imagem

Considerando que toda função f de *A* em *B* é uma relação binária, então f tem um domínio e uma imagem.

Domínio

Chamamos de domínio o conjunto *D* dos elementos $x \in A$ para os quais existe $y \in B$ tal que $(x, y) \in f$. Como, pela definição de função, todo elemento de *A* tem essa propriedade, temos nas funções:

domínio = conjunto de partida

isto é,

$$D = A.$$

[3] As definições apresentadas nos itens 2.3, 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.3.5, 2.3.6 e 2.3.7 foram retiradas do livro Fundamentos de Matemática Elementar - V.1 dos autores Gelson Iezzi e Carlos Murakami.
[4] Em todo o nosso estudo de funções, fica estabelecido que A e B são conjuntos formados por números reais, isto é, A e B contidos em $\mathbb{R}$.

Imagem

Chamamos de imagem o conjunto *Im* dos elementos $y \in B$ existe $x \in A$ tal que $(x, y) \in f$, portanto:

imagem é subconjunto do contradomínio

isto é,

$$Im \subset B.$$

Notemos que, feita a representação cartesiana da função f, temos:

Domínio: *(D)* é o conjunto das abscissas dos pontos tais que as retas verticais conduzidas por esses pontos interceptam o gráfico de f, isto é, é o conjunto formado por todas as abscissas dos pontos do gráfico de f.

Imagem: *(Im)* é o conjunto das ordenadas dos pontos tais que as retas horizontais conduzidas por esses pontos interceptam o gráfico de f, isto é, é o conjunto formado por todas as ordenadas dos pontos do gráfico de f.

Domínio das funções numéricas

As funções que apresentam maior interesse na Matemática são as funções numéricas, isto é, aquelas em que o domínio *A* e o contradomínio *B* são subconjuntos de $\mathbb{R}$. As funções numéricas são também chamadas funções reais de variável real.

Observemos que uma função f fica completamente definida quando são dados o seu domínio *D*, o seu contradomínio e a lei de correspondência $y = f(x)$. Quando nos referirmos à função f e damos apenas a sentença aberta $y = f(x)$ que a define, subentendemos que *D* é o conjunto dos números reais *x* cujas imagens pela aplicação f são números reais, isto é, *D* é formado por todos os números reais *x* para os quais é possível calcular $f(x)$.

$x \in D \Leftrightarrow f(x) \in \mathbb{R}$

2.3.1 FUNÇÃO AFIM

Uma aplicação de $\mathbb{R}$ em $\mathbb{R}$ recebe o nome de *função afim* quando a cada $x \in \mathbb{R}$ associa o elemento $(ax + b) \in \mathbb{R}$ em que a com $a \neq 0$ e b são números reais dados.

$$f(x) = ax + b \ (a \neq 0)$$

2.3.2 FUNÇÃO QUADRÁTICA

Uma aplicação f de $\mathbb{R}$ em $\mathbb{R}$ recebe o nome de *função quadrática* ou Polinomial do 2º grau quando associa a cada $x \in \mathbb{R}$ o elemento $(ax^2 + bx + c) \in \mathbb{R}$, em que a, b e c são números reais dados e $a \neq 0$.

$$f(x) = ax^2 + bx + c \quad (a \neq 0)$$

2.3.3 FUNÇÃO INJETORA

Uma função f de A em B é injetiva se, e somente se, quaisquer que sejam x_1 e x_2 de A, se $x_1 \neq x_2$ então $f(x_1) \neq f(x_2)$.

Em símbolos:

$f: A \to B$

f é injetiva $\Longrightarrow (\forall\, x_1,\ x_1 \in A, \forall\, x_2,\ x_2 \in A\,)(x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2))$

Notemos que a definição proposta é equivalente a: uma função f de A em B é injetora se, e somente se, quaisquer que sejam x_1 e x_2 de A, se $f(x_1) = f(x_2)$, então $x_1 = x_2$.

$f: A \to B$

f é injetora $\Longrightarrow (\forall\, x_1,\ x_1 \in A, \forall\, x_2,\ x_2 \in A\,)(f(x_1) = f(x_2) \Longrightarrow x_1 = x_2)$

Em lugar de dizermos " f é uma função injetora de A em B" poderemos dizer " f é uma injeção de A em B".

2.3.4 FUNÇÃO SOBREJETORA

Uma função f de A em B é sobrejetora se, e somente se, para todo *y* pertencente a *B* existe um elemento *x* pertencente a *A* tal que f (x) = *y*.

Em símbolos:

$f: A \to B$

f é sobrejetora $\Leftrightarrow \forall\, y,\ y \in B, \exists x,\ x \in A \mid f(x) = y$

Notemos que f: $A \to B$ é sobrejetora se, e somente se, *Im (f) = B*.

$f: A \to B$

f é sobrejetora $\Leftrightarrow$ *Im (f) = B*

Em lugar de dizermos " f é uma função sobrejetora de *A* em *B*" poderemos dizer " f é uma sobrejeção de *A* em *B*".

2.3.5 FUNÇÃO BIJETORA

Uma função f de *A* em *B* é bijetora se, e somente se, f é sobrejetora e injetora.

Em símbolos:

$f: A \to B$

f é bijetora = f é sobrejetora e injetora

A definição acima é equivalente a: uma função f de *A* em *B* é bijetora se, e somente se, para qualquer elemento *y* pertencente a *B,* existe um único elemento *x* pertencente a *A* tal que $f(x) = y$.

$f: A \to B$

f é bijetora $\Leftrightarrow \forall\, y,\ y \in B, \exists x,\ x \in A \mid f(x) = y$

Em lugar de dizermos "f é uma função bijetora de A em B" poderemos dizer "f é uma bijeção de A em B"

2.3.6 FUNÇÃO INVERSA

Se f é uma função bijetora de A em B, a relação inversa de f é uma função de B em A que denominamos função inversa de f e indicamos por f^{-1}, tal que $f^{-1}: B \to A$.

> $y \in B$ é tal que $f^{-1}(y) = x$ onde x é o único elemento em A que satisfaz $f(x) = y$.

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

Demonstração:

i. Se f^{-1} é uma função de B em A, então f é bijetora.

- Para todo $y \in B$ existe um $x \in A$ tal que $f^{-1}(y) = x$, isto é, $(y, x) \in f^{-1}$, ou ainda, $(x, y) \in f$. Assim f é sobrejetora.

- Dados $x_1 \in A$ e $x_2 \in A$, com $x_1 \neq x_2$, se tivermos $f(x_1) = f(x_2) = y$ resultará em $f^{-1}(y) = x_1$ e $f^{-1}(y) = x_2$, o que é absurdo pois y só tem uma imagem em f^{-1}. Assim $f(x_1) \neq f(x_2)$ e f é injetora.

ii. Se f é bijetora, então f^{-1} é uma função de B em A.

- Como f é sobrejetora, para todo $y \in B$ existe um $x \in A$ tal que $(x, y) \in f$; portanto, $(y, x) \in f^{-1}$.

- Se $y \in B$, para duas imagens x_1 e x_2 em f^{-1}, vem: $(y, x_1) \in f^{-1}$ e $(y, x_2) \in f^{-1}$; portanto, $(x_1, y) \in f$ e $(x_2, y) \in f$.

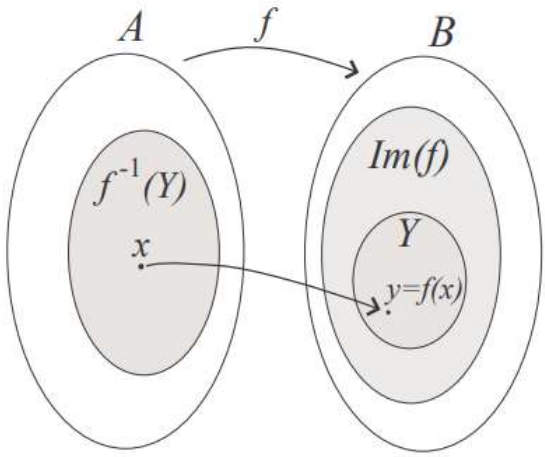
Como f é injetora, resulta $x_1 = x_2$.

2.3.7 IMAGEM INVERSA DE UM CONJUNTO

Sejam $f : A \to B$ uma função e $Y \subseteq B$, chama-se imagem inversa de Y pela função f ao conjunto $f^{-1}(Y)$ formado por todos os $x \in A$ tais que $f(x) \in Y$. Simbolicamente,

$$f^{-1}(Y) = \{x \in A: f(x) \in Y\} \quad ou \quad f^{-1}(f(X)) = \{x \in A \mid f(x) \in f(X)\}$$

Figura 10 - Imagem Inversa do conjunto Y ⊆ B pela função f: A → B.



Fonte: https://www.ime.unicamp.br/~valle/PastCourses/Licao8.pdf

A Figura anterior apresenta uma interpretação visual do conjunto $Y \subseteq B$ pela função $f: A \to B$.

A partir da definição de imagem inversa de um conjunto podemos escrever as seguintes equivalências lógicas:

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

$$x \notin f^{-1}(Y) \Leftrightarrow f(x) \notin Y.$$

CAPÍTULO 3
O CAMINHO PERCORRIDO

Neste capítulo apresentamos o caminho percorrido para a realização do nosso estudo. Para isso, descrevemos o passo a passo das ações realizadas, o contexto em que a proposta foi desenvolvida, como coletamos os dados, o instrumento dessa coleta de dados e destacamos como a proposta conversa com a fundamentação teórica apresentada no Capítulo 2.

Destacamos que toda a aplicação da atividade foi gravada utilizando o aplicativo OBS Studio, o que permitiu retomarmos sempre que foi preciso para rever o ocorrido, as falas dos alunos e ainda transcrevermos alguns trechos.

3.1 OS PRIMEIROS PASSOS

O tema CRIPTOGRAFIA foi escolhido porque, enquanto professor de matemática da Educação Básica, sempre gostei muito de trabalhar com funções e também de associar aplicações aos conteúdos com os quais estou trabalhando. Em conversa com a professora Drª Ana Lúcia da Silva, docente de uma das disciplinas do curso, fui apresentado a criptografia, cujo assunto envolve enviar e receber mensagens, vi nesse tipo de atividades de codificar e decodificar uma associação direta com funções e me interessei.

Para iniciar este estudo realizei, junto a orientadora, algumas tarefas de criptografar e decifrar mensagens.

Em seguida, realizei leituras sobre criptografia e sua história, em dissertações e teses, foram selecionados trabalhos principalmente do banco de dissertações do PROFMAT e, no Google, realizando buscas com palavras chaves que envolvem a criptografia, por exemplos, “dissertação criptografia, codificar decodificar, criptografia atividades voltadas para o ensino Médio e Fundamental, criptografia e funções. As informações que foram consideradas relevantes foram organizados no texto que compõe parte do Capítulo 1.

Depois desta ação realizei um estudo a respeito do conteúdo matemático de funções, os quais eu considerava estar diretamente ligado às atividades que seriam elaboradas, como base para isso analisei outras propostas

apresentadas nas dissertações estudadas para conhecer mais a respeito de criptografia, sua história e aplicações.

O próximo passo deste estudo foi elaborar duas questões que julgávamos que seriam apropriadas para alunos dos anos finais do Ensino Fundamental e alunos do Ensino Médio, mais especificamente para trabalhar o assunto de funções. As atividades foram elaboradas para o 9º ano do EF e para o 1ª série do EM, no entanto o trabalho com os códigos, a criptografia, pode ser feito de uma forma menos formal, mais intuitiva até nos anos iniciais. As atividades podem oportunizar o desenvolvimento dos conceitos matemáticos que são utilizados ao codificar e decodificar mensagens, conceitos esses associados aos conteúdos de funções. As duas atividades elaboradas são apresentadas na sequência.

3.2 ATIVIDADE 1

Esta proposta de atividade tem como finalidade a introdução de conteúdos a serem estudados por alunos dos anos finais do EF e alunos do EM associado com aplicações no nosso cotidiano, ou seja, que faz parte da nossa vida, ela vai proporcionalizar, de maneira sucinta, um estudo das funções quadráticas que podem ser utilizadas para a criptografia. Para isto começamos a verificação por meio de uma função quadrática. Consideramos, nesse contexto que a dúvida pode despertar a curiosidade.

Para iniciar as orientações didáticas o pesquisador comenta a importância de manter uma mensagem em segredo e como isto ajuda nos dias em muitas situações.

Exemplo: mensagens enviadas no WhatsApp, transações financeiras, compra e venda de mercadoria (comércio) ou mesmo informações governamentais confidenciais.

A criptografia garante que as mensagens do WhatsApp sejam seguras, é que apenas o emissor e o receptor tenham acesso ao conteúdo original da mensagem. E mais, cada mensagem tem uma nova chave de criptografia, que é excluída assim que uma mensagem é descriptografada.

A atividade consiste em mandar uma mensagem confidencial para outro aluno ou aluna, sem os demais ficarem sabendo, exceto o destinatário.

Na primeira situação vamos utilizar uma função quadrática do tipo $f(x) = ax^2 + bx + c$, para definir a função. Devemos escolher o conjunto do domínio e do contradomínio, vamos definir o domínio no conjunto dos Inteiros no intervalo de [–12; 13] e o contradomínio nos reais.

A definição do domínio da função associada ao nosso alfabeto gera uma correspondência entre cada elemento com uma letra do alfabeto, segue a figura de correspondência.

A	**–12**	**N**	**1**
B	**–11**	**O**	**2**
C	**–10**	**P**	**3**
D	**–9**	**Q**	**4**
E	**–8**	**R**	**5**
F	**–7**	**S**	**6**
G	**–6**	**T**	**7**
H	**–5**	**U**	**8**
I	**–4**	**V**	**9**
J	**–3**	**W**	**10**
K	**–2**	**X**	**11**
L	**–1**	**Y**	**12**
M	**0**	**Z**	**13**

Associação do domínio da função com o nosso alfabeto

Após a definição do domínio vamos escolher a função para gerenciar a codificação que no caso será $f(x) = x^2 – 1$. Assim, ao codificar cada letra do alfabeto na referida função chegaremos aos seguintes valores.

Quadro 1 - Correspondência entre o domínio da função e as letras do alfabeto aplicado na função quadrática $f(x) = x^2 – 1$.

Letra do Alfabeto	***Correspondência entre os números associados a cada letra aplicada na função f(x)***	***Número gerado***
Letra A	$f(x) = (-12)^2 –1 = 144 – 1 = 143$	143
Letra B	$f(x) = (-11)^2 – 1 = 121 – 1 = 120$	120
Letra C	$f(x) = (-10)^2 – 1 = 100 – 1 = 99$	99
Letra D	$f(x) = (-9)^2 – 1 = 81 – 1 = 80$	80
Letra E	$f(x) = (-8)^2 – 1 = 64 – 1 = 63$	63
Letra F	$f(x) = (-7)^2 – 1 = 49 – 1 = 48$	48
Letra G	$f(x) = (-6)^2 – 1 = 36 – 1 = 35$	35
Letra H	$f(x) = (-5)^2 – 1 = 25 – 1 = 24$	24
Letra I	$f(x) = (-4)^2 – 1 = 16 – 1 = 15$	15
Letra J	$f(x) = (-3)^2 – 1 = 9 – 1 = 8$	8
Letra K	$f(x) = (-2)^2 – 1 = 4 – 1 = 3$	3
Letra L	$f(x) = (-1)^2 – 1 = 1 – 1 = 0$	0
Letra M	$f(x) = (0)^2 – 1 = 0 – 1 = – 1$	– 1
Letra N	$f(x) = (1)^2 – 1 = 1 – 1 = 0$	0
Letra O	$f(x) = (2)^2 – 1 = 4 – 1 = 3$	3
Letra P	$f(x) = (3)^2 – 1 = 9 – 1 = 8$	8
Letra Q	$f(x) = (4)^2 – 1 = 16 – 1 = 15$	15

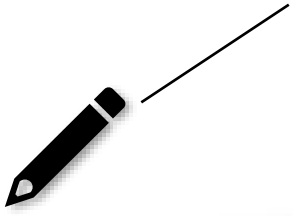
Letra R	$f(x) = (5)^2 - 1 = 25 - 1 = 24$	24
Letra S	$f(x) = (6)^2 - 1 = 36 - 1 = 35$	35
Letra T	$f(x) = (7)^2 - 1 = 49 - 1 = 48$	48
Letra U	$f(x) = (8)^2 - 1 = 64 - 1 = 63$	63
Letra V	$f(x) = (9)^2 - 1 = 81 - 1 = 80$	80
Letra W	$f(x) = (10)^2 - 1 = 100 - 1 = 99$	99
Letra X	$f(x) = (11)^2 - 1 = 121 - 1 = 120$	120
Letra Y	$f(x) = (12)^2 - 1 = 144 - 1 = 143$	143
Letra Z	$f(x) = (13)^2 - 1 = 169 - 1 = 168$	168

Agora pode-se começar a criptografar.

Exemplo de uma frase para a atividade em sala de aula.

G	O	S	T	O		D	E		V	O	C	E
35	3	35	48	3		80	63		80	3	99	63

Depois do processo de criptografar a mensagem é destinada para o interessado que vai tentar decifrar a mensagem confidencial.



Após os alunos decifrarem a mensagem, o que pode ocorrer de diversas maneiras, o professor discute com o grande grupo as estratégias utilizadas pelos alunos e associa, ou sugere, com a “função” que faz o caminho inverso, ou seja, o caminho do código numérico para a respectiva letra do alfabeto.

Neste momento explora-se a definição de imagem inversa que faz a volta, contradomínio para o domínio.

Assim a imagem inversa da f(x) = x² – 1, é dada por $f^{-1}(f(x))$ que vai ser utilizada para decifrar a mensagem criptografada. Acompanhe o processo:

y = 35 $\longrightarrow\ f^{-1}(35) = \sqrt{35+1} = \sqrt{36} \longrightarrow \{-6, 6\}$

y = 3 $\longrightarrow f^{-1}(3) = \sqrt{3+1} = \sqrt{4} \longrightarrow \{-2, 2\}$

y = 48 $\longrightarrow\ f^{-1}(48) = \sqrt{48+1} = \sqrt{49} \longrightarrow \{-7, 7\}$

y = 80 $\longrightarrow\ f^{-1}(80) = \sqrt{80+1} = \sqrt{81} \longrightarrow \{-9, 9\}$

y = 63 $\longrightarrow\ f^{-1}(63) = \sqrt{63+1} = \sqrt{64} \longrightarrow \{-8, 8\}$

y = 99 $\longrightarrow\ f^{-1}(99) = \sqrt{99+1} = \sqrt{100} \longrightarrow \{-10, 10\}$

Chegamos em um impasse, ou seja, não conseguimos ter certeza da mensagem recebida, pois, no processo da volta não temos uma única letra correspondente vinculada ao número, gerando assim um problema: a mensagem decifrada poderia ter várias combinações possíveis e diferentes.

Exemplo:

Mensagem criptografada:

35	**3**	**35**	**48**	**3**		**80**	**63**		**80**	**3**	**99**	**63**

Decifrando a mensagem através da imagem inversa, temos os seguintes resultados:

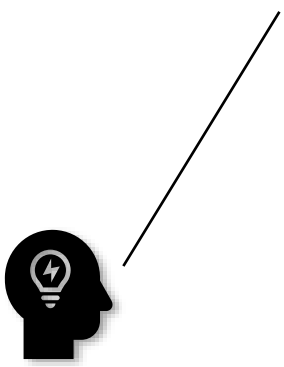
–6	**–2**	**–6**	**–7**	**–2**		**–9**	**–8**		**–9**	**–2**	**–10**	**–8**
6	**2**	**6**	**7**	**2**		**9**	**8**		**9**	**2**	**10**	**8**

Respectivas letras associadas os resultados da imagem inversa:

G	K	G	F	K		D	E		D	K	C	E
S	O	S	T	O		V	U		V	O	W	U

O problema é que, o mesmo número recebido leva a duas letras diferentes. Assim fica inviável esta função quadrática para a criptografia, pelo menos com este domínio.

Algumas indagações importantes:



I) O que ocasionou o problema de não conseguir chegar ou voltar em uma única letra?

II) Com a tabela acima conseguimos decifrar a mensagem, mas, tenho certeza que é a mensagem original transmitida? Quantas palavras de 5 letras poderíamos formar somente com o primeiro trecho

$2 . 2 . 2 . 2 . 2 = 32$

III) A escolha dos números associados as letras poderiam ser diferentes?

IV) A escolha da função faz alguma diferença na codificação?

V) Utilizando esta mesma função, poderíamos modificar alguma coisa para ela ser utilizada de maneira correta na criptografia.

3.3 ATIVIDADE 2

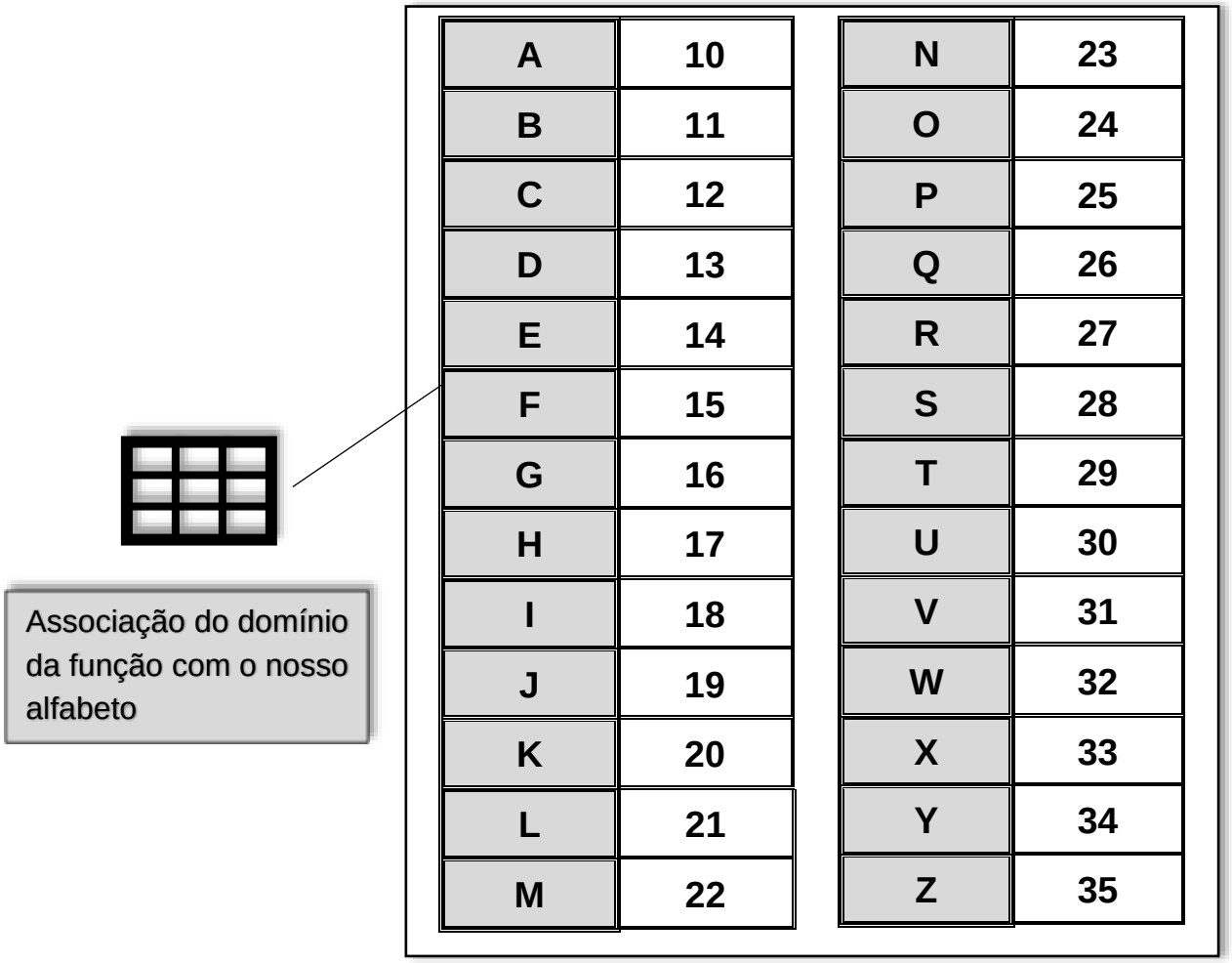
Dando continuidade às reflexões que a atividade 1 proporcionou e, com a intenção de esclarecer dúvidas levantadas nessas reflexões, uma segunda proposta é feita; agora com uma função do primeiro grau, mas através de um desafio: aquele que conseguir decifrar a mensagem do outro mostrando a regra ou a função que foi utilizado para codificar a mensagem em um menor tempo vence o desafio.

A atividade consiste primeiramente em dividir os alunos de uma turma em trios, quartetos ou até quintetos, dependendo da quantidade de alunos da turma. Em seguida os grupos devem cifrar uma mensagem escolhida.

Na primeira fase os grupos irão criar uma regra (função do 1º grau) para codificar a mensagem. Então os grupos trocam a mensagem codificada, o professor organiza para que todos os grupos tenham que decodificar a mensagem de outro grupo. Recebida a mensagem, os grupos devem tentar decodificá-la, ou seja, tem que achar a função que gerou a sequência de letras enviada.

Um exemplo na primeira fase:

Em acordo com todos os componentes do grupo, o domínio escolhido foi no conjunto dos Inteiros no intervalo de [10, 35] e a função do 1º grau foi definida por f(x) = 2x – 1 (um exemplo) e todas as letras do alfabeto foram criptografas para poder codificar a mensagem escolhida. Assim escolhe-se o primeiro número do domínio a associa-o a primeira letra do alfabeto, criando figura.



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

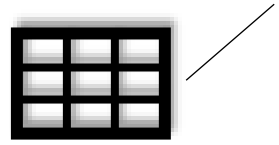
Codificando as letras através da função escolhida f(x) = 2.x – 1, temos:

Quadro 2 - Correspondência entre o domínio da função e as letras do alfabeto aplicado na função f(x) = 2x – 1.

Letra do Alfabeto	*Correspondência entre os números associados a cada letra aplicada na função f(x)*	*Número gerado*
Letra A	f(x) = 2.(10) –1 = 20 – 1 = 19	19
Letra B	f(x) = 2.(11) –1 = 22 – 1 = 21	21
Letra C	f(x) = 2.(12) –1 = 24 – 1 = 23	23
Letra D	f(x) = 2.(13) –1 = 26 – 1 = 25	25

Letra E	f(x) = 2.(14) –1 = 28 – 1 = 27	27
Letra F	f(x) = 2.(15) –1 = 30 – 1 = 29	29
Letra G	f(x) = 2.(16) –1 = 32 – 1 = 31	31
Letra H	f(x) = 2.(17) –1 = 34 – 1 = 33	33
Letra I	f(x) = 2.(18) –1 = 36 – 1 = 35	35
Letra J	f(x) = 2.(19) –1 = 38 – 1 = 37	37
Letra K	f(x) = 2.(20) –1 = 40 – 1 = 39	39
Letra L	f(x) = 2.(21) –1 = 42 – 1 = 41	41
Letra M	f(x) = 2.(22) –1 = 44 – 1 = 43	43
Letra N	f(x) = 2.(23) –1 = 46 – 1 = 45	45
Letra O	f(x) = 2.(24) –1 = 48 – 1 = 47	47
Letra P	f(x) = 2.(25) –1 = 50 – 1 = 49	49
Letra Q	f(x) = 2.(26) –1 = 52 – 1 = 51	51
Letra R	f(x) = 2.(27) –1 = 54 – 1 = 53	53
Letra S	f(x) = 2.(28) –1 = 56 – 1 = 55	55
Letra T	f(x) = 2.(29) –1 = 58 – 1 = 57	57
Letra U	f(x) = 2.(30) –1 = 60 – 1 = 59	59
Letra V	f(x) = 2.(31) –1 = 62 – 1 = 61	61
Letra W	f(x) = 2.(32) –1 = 64 – 1 = 63	63
Letra X	f(x) = 2.(33) –1 = 66 – 1 = 65	65
Letra Y	f(x) = 2.(34) –1 = 68 – 1 = 67	67
Letra Z	f(x) = 2.(35) –1 = 69 – 1 = 69	69

Após a codificação as letras do alfabeto estarão associadas aos seguintes números:



Associação entre as letras e os números após a codificação

A	19	N	45
B	21	O	47
C	23	P	49
D	25	Q	51
E	27	R	53
F	29	S	55
G	31	T	57
H	33	U	59
I	35	V	61
J	37	W	63
K	39	X	65
L	41	Y	67
M	43	Z	69

Com o alfabeto codificado podemos então cifrar as mensagens. Segue um exemplo.

COMPARTILHAR

MENSAGEM	C	O	M	P	A	R	T	I	L	H	A	R
Associação com números escolhidos	12	24	22	25	10	27	29	18	21	17	10	27
Mensagem cifrada a partir da função	23	47	43	49	19	53	57	35	41	33	19	53

Com este código (sequência de números), na segunda fase, o grupo que receber essa mensagem tem que decifrar a mensagem.

Mensagem cifrada a partir da função	**23**	**47**	**43**	**49**	**19**	**53**	**57**	**35**	**41**	**33**	**19**	**53**
Mensagem cifrada (letras)												

Algumas observações ou características dos códigos, desse exemplo, que eles podem verificar e que vão ajudar na decodificação.

- todos são ímpares;
- sequência matemática que gera um número ímpar;
- o menor é o dezenove;
- o maior é o 57;
- dois números consecutivos ímpares que constam na sequência.

Ao final da segunda fase, após os grupos chegarem à função, pode-se conversar a respeito da diferença entre a Atividade 1 e a Atividade 2.

Uma orientação aos professores é que se os alunos não chegarem a nenhuma caracterização, os professores podem fazem as seguintes perguntas:

1) Olhando para os números desta sequência, o que vocês podem observar?
2) Você consegue identificar qual é o menor número e qual é o maior?
3) Existem números consecutivos nesta sequência?
4) Existem números consecutivos pares nesta sequência?
5) Existem números consecutivos ímpares nesta sequência?
6) Por que não temos números menores que dezenove e números maiores que cinquenta e sete nesta sequência?

3.4 APLICAÇÃO DA ATIVIDADE 1

Na sequência da elaboração destas atividades, tive a oportunidade de aplicar uma delas com um grupo de pessoas envolvidas na Educação Básica, esse grupo, composto por dez pessoas foi formado de:

- tutores da OBMEP[5] (T1, T2, T3, T4, T5),
- alunos da 1ª série do Ensino Médio de escola pública (A1, A2),
- um professor da Educação Básica (PEB),
- um professor Ensino Superior (PS) e
- o pesquisador.

Por conta da pandemia realizamos o encontro de forma remota via Google Meet e aplicamos a primeira atividade. O capítulo quatro descreve a aplicação da atividade 1.

Além das descrições, para reflexão a respeito da atividade e do desenvolvimento dos alunos, fizemos algumas análises considerando o capítulo dois que apresenta os conteúdos de matemática. Associamos formalmente o conteúdo de funções, parte dessa associação foi comentada com os alunos. Outra parte só foi extraída no momento das descrições e análises, no entanto ela compõe o desenvolvimento da atividade 1.

Lembramos que:
PEB é professor da Educação Básica
T1 é Tutor da OBMEP
T2 é Tutor da OBMEP
T3 é Tutor da OBMEP
T4 é Tutor da OBMEP
T5 é Tutor da OBMEP
A1 é aluno do ensino médio
PS é professora do ensino superior
A2 é aluno do ensino médio

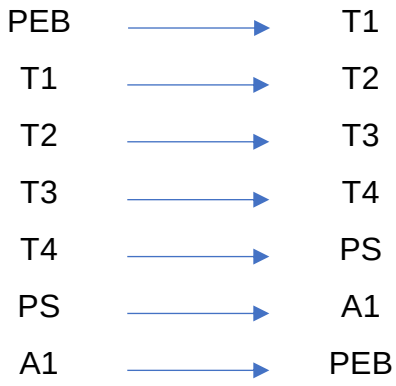
[5] São professores (ex-alunos medalhistas) da OBMEP, que participam do Programa de Iniciação Cientifica (PIC), que monitoram alunos medalhistas dos níveis 1, 2 e 3 das olimpíadas de matemática.

CAPÍTULO 4
DESCRIÇÃO E ANÁLISE DAS ATIVIDADES

A atividade 1 teve o objetivo de inserir os alunos no universo de mensagens criptografadas.

Para esse relato foi organizada uma aula remota com cinco tutores da OBMEP, dois alunos do 1º ano do Ensino Médio, de escola pública, um professor da Educação Básica, também de escola pública e um professor convidado do ensino superior. Vamos nomear cada um dos participantes pelas siglas PEB, T1, T2, ... T5. A aula ocorreu no Google Meet e teve a duração de aproximadamente 2h30.

Para iniciar foi mandada a atividade pelo WhatsApp no formato Word. Os participantes tiveram um tempo para ler o enunciado da questão. Em seguido foi pedido para que cada um escolhesse uma palavra e codificasse-a. Como eram poucos os participantes, foi organizado que a troca de mensagens seria da seguinte forma:



Dessa maneira, cada um teria que decifrar a mensagem de outro participante. Em seguido utilizamos o chat para encaminhar os códigos. Um pouco depois da distribuição, dois participantes entraram na aula, denominamo-los de A2 e T5, eles participaram ativamente na aula.

Com exceção de um, aproximadamente em 10 min, os participantes já haviam encaminhado a mensagem; ocorreu que, ao abrir o arquivo da atividade a função não apareceu, e T1 então acabou que fazendo o código apenas utilizando a tabela.

A palavra escolhida por T1 foi TERRA PRETA e, o primeiro código que ele mandou foi 7; -8; 5; 5; -12; 3; 5; -8; 7; -12. T1 logo desconfiou que tinha alguma

coisa errada com a sua codificação. Ele percebeu que somente a sua mensagem tinha números negativos. Então T2 o advertiu a respeito disse e eles mesmos concluíram que ele não tinha visto a função de entrada. Com o alerta essa questão foi solucionada rapidamente.

Quando todos já haviam decodificado a mensagem sob sua incumbência o pesquisador da atividade foi perguntando um a um qual era a palavra recebida e se o decodificador tinha tido algum problema.

Observe no quadro abaixo os códigos recebidos por cada um dos participantes e a sua decodificação:

Quadro 3 - Códigos e palavras propostos por cada participantes

PEB	8; 24; 3; 48; -1; 143; 48	PROFMAT
T1	3; 24; 35; 143; 0; 15; 99; 3	ORGÂNICO
T2	8; 143; 0; 80; 63; -1; 15; 143	PANDEMIA
T3	35; 143; 99; 3; 0; 143	SACOLA
T4	15; 63; 143; 48; 24; 3; 99; 63; 0; 48; 3; 35	QUATROCENTOS
T5	80; 15; 143; 8; 143; 24	VIAJAR
A1	48; 63; 0; 15; 99; 15; 80; 143; 80; 63	FELICIDADE
A2	168; 63; 120; 24; 143	ZEBRA

Fonte: o autor

O participante T5, como podemos observar na tabela acima, não apresentou uma palavra, porém ele decodificou as palavras de outros participantes, por não saber das regras, acabou colocando algumas delas no chat antes do momento da apresentação das decodificações.

No decorrer do desenvolvimento e com a mensagem sendo transmitidas no chat da aula, conforme iam terminando e esperando os demais, alguns participantes começaram a trocar outras mensagens, mas com um grau maior de dificuldade para decifrar, como por exemplo o T4 para T2, (3; 80; 3; 63; 35; 63; 48; 143; 24; 15; 143; 0; 143) que significa OVO VEGETARIANA, outro foi o T5 que mandou para o grupo duas mensagens cujos códigos são 99; 3; 80; 15; 35; 3 e -1;

63; 0; 48; 15; 24; 143 com os significados de CODIGO e MENTIRA. Com isso pudemos perceber a interação dos participantes com a atividade proposta.

Com a apresentação das mensagens surgiram algumas brincadeiras e algumas suposições, eles notaram que não tinham certeza com relação a palavra, por exemplo, quando perguntado a T1 se ele tinha decifrado a mensagem, a resposta foi: *"sim... é, quer dizer, eu acho né, porque tem várias possibilidades"* tivemos também o T4 que respondeu *"a palavra que T3 me mandou foi SACOLA ou GACONA, talvez alguma coisa assim..."* já no momento de A1 relatar, ocorreu um problema pois a palavra criptografada era VIAJAR e foi decifrada como VIAPAR, surgindo um impasse.

Na sequência o pesquisador questionou os alunos do 1º ano do Ensino Médio a respeito da estratégia que eles utilizaram para decodificar a mensagem. A fala do T5 foi "*eu peguei apresentei, eu... tipo tem 99 eu sei que mais 1 é o quadrado de 100 que é 10 .... sei que na verdade 16 é quadrado de 4 ou -4 dependendo... daí a gente vai ver como se encaixa... aí eu acho que entendi o que vocês quiseram dizer .... tipo eu escrevi VIAJAR mas para ela deu VIAPAR... aí pode ter duas possíveis, como tem menos e mais"*.

Matematicamente podemos escrever:

$f(x) = x^2 - 1$, considerando $f(x) = 99, temos$:

$$99 + 1 = x^2$$

$$\sqrt{100} = x$$

$$x = 10$$

Explorando o raciocínio de T5

T5 disse que: "*o quadrado de 100 que é 10",* essa afirmação não está correta.

A afirmação deveria ser: a raiz quadrada de 100 é 10.

Na sequência diz: "*na verdade 16 é quadrado de 4 ou -4 dependendo....".* $(4)^2 = 16$ *e* $(-4)^2 = 16$. A participante ainda diz: *dependendo*. O que ela pode querer dizer? Inferimos que T5 estivesse referindo-se a utilização das letras I e Q.

A discussão a respeito das palavras VIAJAR e VIAPAR ainda renderam algumas reflexões. T5 comentou: *"então talvez se a gente só usasse ou só número negativo ou só positivo ....resolveríamos isso..."* levando em consideração

essa colocação de T5, o pesquisador diz: "*como poderíamos trabalhar só com os positivos ou só com os negativos*"? PEB respondeu: *"modificar o domínio"* e T5 também concordou: *"modificar o domínio da função".*

A alteração proposta por PEB e T5 é válida, pois se restringirmos o domínio e o contradomínio da função, então esta pode admitir a função inversa. Por exemplo se o domínio for definido somente nos positivos ou somente nos negativos isto só geraria um respectivo elemento no contradomínio. Temos também que nos preocuparmos com o contradomínio, pois ele teria que ser constituído somente pela imagem do domínio, ou seja, $CD(F) = Im(F)$, onde

$$D(f) = \{1, 2, 3, 4, \dots, 25, 26\}$$

$$CD(f) = \{0, 3, 8, 15, \dots, 624, 675\}$$

Assim, teríamos:

$$f(1) = 1^2 - 1 = 1 - 1 = 0$$

$$f(2) = 2^2 - 1 = 4 - 1 = 3$$

$$f(3) = 3^2 - 1 = 9 - 1 = 8$$

$$f(4) = 4^2 - 1 = 16 - 1 = 15$$

...

$$f(25) = 25^2 - 1 = 625 - 1 = 624$$

$$f(26) = 26^2 - 1 = 676 - 1 = 675$$

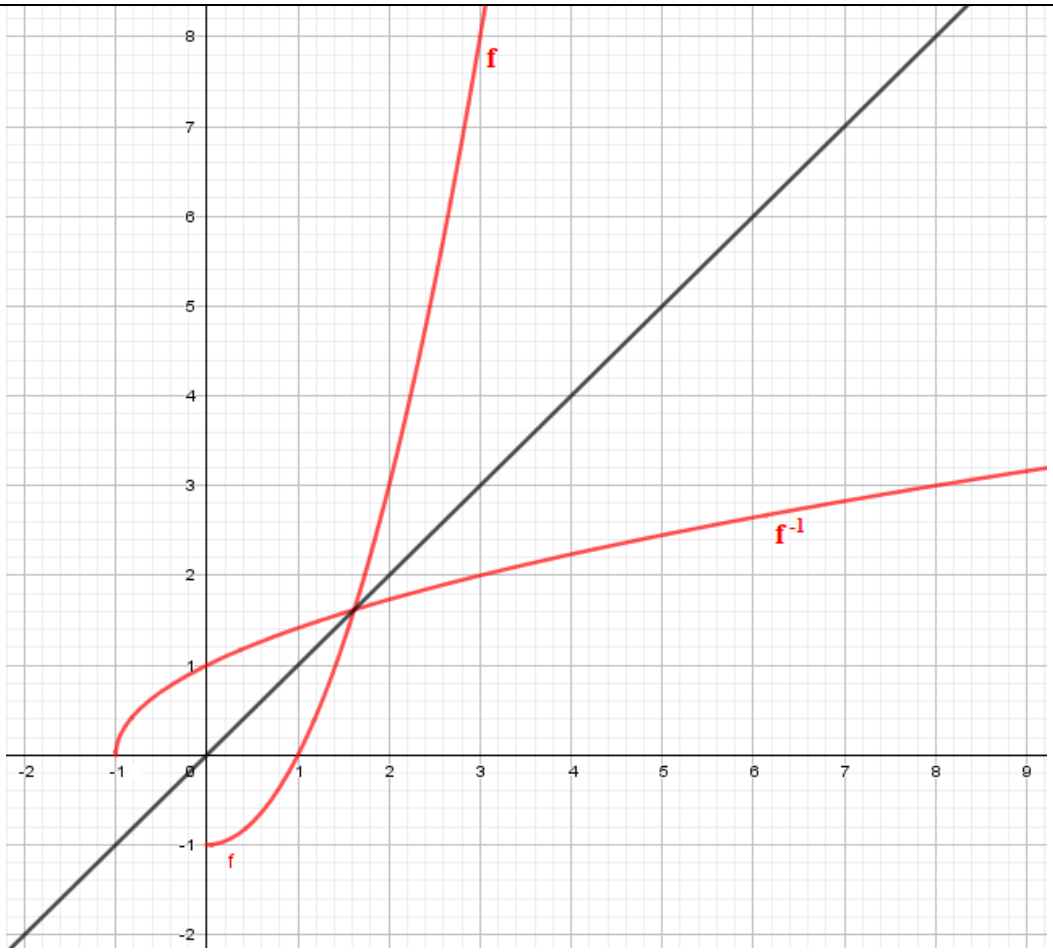
Outra possibilidade, seria somente mudar o domínio para os números negativos e o contradomínio continuaria o mesmo. Assim, teríamos:

$$D(f) = \{-26, -25, \dots, -4, -3, -2, -1\}$$

$$CD(f) = \{0, 3, 8, 15, \dots, 624, 675\}$$

Nestas duas possibilidades teríamos funções bijetoras, consequentemente função inversa.

Como por exemplo a seguintes representações gráficas:



Observem que o gráfico da função f^{-1} será sempre simétrico ao gráfico da função f em relação à reta y = x, ou seja, simétrico a bissetriz dos quadrantes 1 e 3, temos também o domínio definido para x ≥ 0 assim como o contradomínio e a imagem para y ≥ – 1.

Quanto a maneira de calcular para codificar a mensagem tivemos os seguintes comentários: A2 disse, *"eu pegava os números codificados... eu somava um e já fazia a raiz quadrada e colocava os números só positivo, depois eu ia na tabela e pegava os negativos e os positivos daquele número, para ter as duas possibilidades... assim era um pouquinho mais rápido de fazer".* Essas respostas instigou a seguinte pergunta: por que vocês achavam que tinham que somar um e fazer a raiz quadrada?

Matematicamente podemos escrever:

$Se\ f(x) = x^2 - 1$, para codificar ele substituiu o número referente a letra, elevou ao quadrado e subtraiu 1. Entendemos que para decodificar ele utiliza as operações

inversas, ou seja, soma um e extrai a raiz quadrado. Essa “regra” é amplamente trabalhada nos anos finais do Ensino Fundamental, quando o professor ensina a resolução de equações, exemplo:

$2x + 5 = 3$ (pelo princípio de equivalência, ao adicionarmos o mesmo número a cada um dos membros da equação, eles ainda permanecem equivalentes, neste exemplo somamos (-5) em ambos os membros da equação).

$$2x + 5 - 5 = 3 - 5$$

$2x = -2$ (pelo princípio de equivalência, ao multiplicarmos o mesmo número a cada um dos membros da equação, eles ainda permanecem equivalentes, neste exemplo multiplicamos por $\left(\frac{1}{2}\right)$ em ambos os membros da equação).

$$2x \cdot \left(\frac{1}{2}\right) = -2 \cdot \left(\frac{1}{2}\right)$$

$$x = -1$$

T5 responde: *“porque x ao quadrado menos um... então vai ser o quadrado de alguma coisa menos um .... então o número de f seria o quadrado, o f seria um número elevado ao quadrado daqueles que estavam lá”*

Exemplo:

8; 24; 3; 48; -1; 143; 48 se adicionarmos 1 a cada termo, teremos

9; 25; 4; 49; 0; 144; 49. Dessa forma, todos os termos são quadrados perfeitos.

E ainda diz: “*o f seria um número elevado ao quadrado daqueles que estavam lá”....* isso quer dizer: 3; 5; 2; 7; 0; 12; 7.

Na sequência A2 também descreve o que ele fez: *“porque o resultado... porque o número que a gente tem que decodificar é f(x) então a gente tem que colocar este número no lugar de f(x), igual a x ao quadrado menos um e fazer o processo para descobrir o x”.*

O pesquisador da atividade pergunta se eles sabiam como chamava tecnicamente este processo para achar a mensagem, T5 disse *“não”* e A2 falou: *“eu chutaria função inversa, mas eu acho que não é... porque função inversa você pega o*

y e coloca no lugar de x, só que eu vi isto no ano passado então eu não lembro direito se vai dar o resultado que eu quero ... deixa eu ver se vai dar... não, vai dar certo... porque a função inversa é quando você eleva a menos um não é" então, o pesquisador comentou que f elevado a menos um (f^{-1}) é somente uma notação da função inversa.

Após o surgimento de indagações e experiências apresentadas nas falas sobre função inversa, o pesquisador faz um breve comentário dizendo que a função e o domínio escolhidos para a atividade não possui função inversa. Em seguida anuncia que uma função para ser inversível tem que apresentar duas propriedades, sendo a primeira que cada elemento do domínio tem que estar associado a um único elemento do contradomínio, ou seja, não pode ter dois elementos do domínio associado a um único elemento do contradomínio. A segunda propriedade é que cada elemento do contradomínio tem que estar associado a um elemento do domínio, introduzindo assim função injetiva, função sobrejetiva e função bijetiva.
Trazendo o rigor matemático temos as seguintes definições:

Função:
Diz-se que uma relação f é uma função f de A em B se, e somente se, para todo elemento a ∈ A existe um único elemento b ∈ B tal que (a; b) ∈ f.
Em outros termos:
Uma função f de A em B é um conjunto de pares ordenados (a, b) tais que a cada elemento a ∈ A corresponde um, e somente um, elemento b ∈ B.

Domínio:
Chama-se domínio ou campo de definição de uma função f de A em B o conjunto dos primeiros elementos a dos pares ordenados (a, b) que pertencem a f. Representa-se por $D(f)$.

Contradomínio:
Chama-se contradomínio de uma função f de A em B o conjunto dos segundos elementos b dos pares ordenados (a, b) que pertencem a f. Representa-se $CD(f)$.

Função:

Dados dois conjuntos *A* e *B* ∈ $\mathbb{R}$, não vazios, uma função $f: A \longrightarrow B$ é uma relação que associa a cada elemento x ∈ A um único elemento *y* ∈ B, $f(x) = y$.

A é chamado domínio ou campo de definição.
B é chamado contradomínio.

$Im\,(f) = \{y \in B \mid \exists \mid x \in A\}$ com $f(x) = y$ é chamado conjunto imagem de *f*.

Função injetiva:
Uma função *f* de *A* em *B* é injetiva se, e somente se, quaisquer que sejam x_1 e x_2 de A, se $x_1 \neq x_2$ então $f(x_1) \neq f(x_2)$.

$f: A \rightarrow B$

f é injetiva $\Longrightarrow (\forall\, x_1,\ x_1 \in A, \forall\, x_2,\ x_2 \in A\,)(x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2))$

Função sobrejetiva:
Uma função *f* de A em B é sobrejetiva se, e somente se, para todo *y* pertencente a *B* existe um elemento *x* pertencente a *A* tal que *f* (x) = *y*.

$f: A \rightarrow B$

f é sobrejetora $\Leftrightarrow (\forall\, y,\ y \in B, \exists x,\ x \in A \mid f(x) = y)$

Função Bijetiva:
Uma função f de *A* em *B* é bijetiva se, e somente se, *f* é injetiva e sobrejetiva.

$f: A \rightarrow B$

f é bijetiva $\Leftrightarrow (\forall\, y,\ y \in B, \exists \mid x,\ x \in A \mid f(x) = y)$

Função inversa:
Chama-se função inversa de uma função bijetora f de A em B a função de B em A que a todo elemento b ∈ B o único elemento a ∈ A cuja imagem pela f é b, ou seja, $f(a) = b$.
Esta função representa-se pela notação f^{-1}. Portanto a função inversa:

$$f^{-1}: B \longrightarrow A$$

Tem por domínio o contradomínio de f e é tal que:

$$f^{-1}(b) = a \Leftrightarrow f(a) = b \quad (\forall a \in A,\ \ \forall b \in B)$$

Imagem inversa:

Seja f uma função de A em B e seja H uma parte de B, onde H ⊂ B. Chama-se imagem inversa ou imagem recíproca de H pela f, o conjunto de todos os elementos de A cujas imagens pela f pertencem a H. Este conjunto representa-se por:

$$f^{-1}(H) = \{x \mid x \in A \ e \ f(x) \in H\}$$

Podemos ter a imagem inversa de um elemento b ∈ B pela f denota-se por $f^{-1}(b)$, e consiste de todos os elementos de A cujas imagens pela f é b, isto é, simbolicamente:

$$f^{-1}(b) = \{x \mid x \in A \ e \ f(x) = b\}$$

Continuando com as considerações e agora com a escrita formal conclui-se juntos com os participantes que a função não é inversível, pois a $f(x) = x^2 - 1$ não é injetora, pois elementos distintos do domínio levam em um mesmo elemento do contradomínio, contradizendo a definição de injetividade, exemplo:

$$x = -10 \Longrightarrow f(-10) = (-10)^2 - 1 = 100 - 1 = 99$$

$$x = 10 \Longrightarrow f(10) = 10^2 - 1 = 100 - 1 = 99$$

e nem sobrejetora, pois como nosso contradomínio foi definido no conjunto dos reais temos elementos que não tem uma correspondência no domínio, como colocado por T5, que sugeriu o número 13, pois se somarmos 1 temos 14 e a raiz quadrada não está no domínio, ou seja, o número que elevado ao quadrado resulta em quatorze. Assim surge a importância da escolha do domínio e do contradomínio de uma função, não importando somente a lei de associação de um conjunto com o outro que compõe uma função, temos que ficar atendo com a escolha destes conjuntos.

Assim, notamos que para realizarmos a criptografia precisamos de um algoritmo que faz essa transição (ida e volta) nos dois conjuntos de maneira única, ou seja, um elemento do domínio só pode estar associado a um único elemento do contradomínio e vice-versa, não dando margem a dupla interpretação como aconteceu na atividade: “VIAPAR” e “VIAJAR”. Fazendo uma observação, supondo que não tivéssemos essa relação de unicidade teríamos uma grande quantidade de possibilidades (anagrama) o que não seria viável para a criptografia, pois como

comentou o pesquisador *"...porque quando a gente manda uma mensagem a forma de enviar uma mensagem e a forma de decrepitar a mensagem, ela não pode dar margem a erros, para o emissor e receptor autorizados, ou seja, na hora que o receptor recebe a mensagem ele não pode achar que esta mensagem poderia ser diferente, tem que ser uma única ..."* , surgiu então, como já foi comentado, como solucionar este problema alterando o domínio e o contradomínio, com as instigações do pesquisador conseguimos mostrar a importância do domínio e do contradomínio adequado. Na sequência houve a exposição e exemplos sobre a diferença entre função inversa e imagem inversa (imagem inversa nem sempre é comentada no estudo de funções), como exemplo temos comentário do pesquisador que no diz *"... agora o que vocês fizeram quando vocês pegavam por exemplo, a eu mando uma mensagem que tem o 63, 63 mais 1 é 64, raiz quadrada de 64, qual é o número quando elevado ao quadrado é igual a 64? (T5 responde 8 e -8) isto são pouquinhos diferentes, isto mesmo mais ou menos 8, não é bem raiz quadrada de 64, pois a raiz quadrada de 64 é 8. Agora qual é o número que quando elevado ao quadrado dá 64, mais ou menos 8, tá, então eu vou ter duas letras associadas, ao 63, coisa que não pode acontecer, o que é isto aqui, é a imagem inversa do 63, são coisas diferentes tá, ..."*

Levando em consideração as falas podemos concluir que o domínio, o contradomínio e a função escolhida $f(x) = x^2 - 1$, matematicamente não é indicada para criptografar, mas com as devidas alterações isto seria possível.

Para terminar foi colocado para os participantes que a ideia desta atividade era para brincar um pouquinho com criptografia e, ao mesmo tempo, introduzir os conceitos de função inversa e imagem inversa e a diferença entre elas, e mostrar que, para toda função, é possível encontrar o conjunto imagem inversa, mas nem toda função possui função inversa. Assim o pesquisador solicitou que eles opinassem sobre esta atividade para trabalhar função inversa e imagem inversa. Os depoimentos foram os seguintes:

Participante T2, *"a eu achei muito legal, é um jeito divertido e eu acho que T5 e A2 acabaram estudando isso sem perceber, e eles mesmo podem ter tirados conclusões sem ninguém dizer a eles ..."*

Participante T3, *"só complementando o que T2 falou, eu acho muito legal quando a gente realiza este tipo de exercício, que os próprios alunos vão definindo os conceitos, e quando a gente passa um conceito e defini, fica aquela coisa de, vou ter que decorar e muitas vezes acaba não fixando, e que nem, neste exato momento A2 e T5 mesmo, eles foram falando: e se eu usar a inversa da função, então eles foram definido o que seria inversa, mas tem que ser injetora para ter uma função inversa, mas o que é bijetora, então a gente já resgatou o conceito de injetora, sobrejetora e talvez fica um pouco vago esse conceito na nossa mente, mas a gente analisando com problema que eles mesmos foram definindo, foram dando os caminhos que a gente tem que seguir, fica mais fácil para gente voltar e lembrar desta definição né, a definição fica mais clara ... isso não foi a outra que deu pronta, foi você que chegou que construiu aquilo né"*

Em seguida A2 pede para fazer o seguinte comentário: *"e quanto você disse que não era uma função inversa eu tentar pensar nisso graficamente, porque não seria? daí eu lembrei que $x^2 - 1$, daria uma parábola, em que teria os resultados com o domínio, positivo e negativo e tudo seria positivo, porque está elevado ao quadrado, e quando eu fui pensar na inversa, seria tipo uma parábola deitada para a direita, só que não poderia ter a parte com y menor que zero ..."*

Esses comentários nos mostram que uma atividade com objetivo somente de introduzir os conceitos de domínio, contradomínio imagem inversa e função inversa, abriu um leque para o aprofundamento no estudo, como a representação gráfica de uma função quadrática no plano cartesiano e a análise de como seria a representação da sua inversa, também foram discutidas algumas propriedades como simétrica e reflexiva.

O participante PEB, professor da Educação Básica, fez seu depoimento após ser perguntado sobre sua opinião em relação a atividade desenvolvida*: "É, como o objetivo de vocês é desconstruir essa ideia mesmo, de função inversa, porque vai haver uma desconstrução, quando você aplicar esta questão, principalmente pela ideia de, a todos eles tem a inversa, não. Dependendo do domínio desta função, se ela é bijetora, existe a inversa, então eu acho que é uma questão muito válida, para você poder aplicar, para fazer justamente esta desconstrução e reforçar os conceitos de bijetora, sobrejetora e injetora e mostrar aquilo que é necessário para*

que exista uma função inversa, então eu gostei bastante da questão, ficou muito bem montada, ficou bem legal". Perguntamos se ele aplicaria nas suas salas, respondeu: *"Sim, com certeza, ficou muito legal"*

Na sequência o pesquisador fez uma pergunta sobre o roteiro da atividade, se foi fácil para eles interpretar e saber o que tinham que fazer, T5 respondeu que surgiu algumas dúvidas no começo, mas depois que começou a decifrar foi entendendo, T2 sugeriu que no passo 3 tem um exemplo aleatório que seria interessante mudar para números do próprio quadro.

Após a execução e análise desta atividade, foi possível a realização de algumas reflexões. Em relação a minha formação profissional, essa atividade envolvendo criptografia me mostrou um caminho diferente para atingir os objetivos traçados, a situação presenciada muitas vezes não acontece em sala de aula, a participação dos alunos muitas vezes é tolhida pelos professores, algumas vezes porque o professor acredita que o pouco tempo que tem com os alunos tem que ser usado para levar o maior número de informações possível.

O relato nos faz perceber que trabalhar a partir das observações ou mesmo dos pensamentos dos alunos permitiu que as ideias da aula fossem dirigidas pelas interpretações dos alunos, a partir das coisas que eles elaboraram, dos códigos criptografados, do que eles pensaram e de como eles fizeram os cálculos. As definições e os formalismos foram inseridos sempre a partir dos que os alunos disseram. Esses fatos nos permitem destacar a importância de o professor trabalhar sempre em sintonia com os alunos, aproveitando e selecionando tudo que os alunos pensam, do que eles compreendem, exemplificando que a aprendizagem ocorre quando os alunos participam ativamente da aula.

CONSIDERAÇÕES FINAIS

Ao pensarmos na educação e na realidade do ensino em nossas escolas, devemos parar e refletir: “nossas práticas estão atingindo significativamente nossos alunos?”, foi com este questionamento que comecei a repensar minhas aulas de matemáticas, e mais: como posso contribuir e ajudar outros educadores nesta busca por uma educação de qualidade?

Foi neste contexto que o PROFMAT entrou nesta trajetória, resolvi fazer minha parte: aprender mais a respeito de Matemática e procurar novas estratégias para o ensino. Para isso, ingressei de novo na universidade, na busca de um suporte e orientações expressivas para sanar todas estas preocupações.

Segundo a última LDB, a lei 9394 das Diretrizes e Bases da Educação Nacional cita:

> O ensino superior tem por finalidade o pleno desenvolvimento do educando, seu preparo para o exercício da cidadania e sua qualificação para o trabalho, bem como deve estimular a criação cultural, o desenvolvimento do espírito científico e do pensamento reflexivo, o incentivo ao trabalho de pesquisa e a investigação científica, com vistas ao desenvolvimento da ciência e da tecnologia e da criação e difusão da cultura, e, desse modo, desenvolver o entendimento do homem e do meio em que vive, além da promoção e da divulgação de conhecimentos culturais, científicos e técnicos que constituem patrimônio da humanidade e comunicação do saber através do ensino, de publicações ou de outras formas de comunicação. Uma das alternativas em busca do conhecimento é o ensino através da pesquisa, desenvolvendo a autonomia dos alunos, instigando-os a questionamentos constantes. (BRASIL, Artigo 43, p.14)

Assim, após estudos, orientações e interação com a comunidade acadêmica, essa proposta tomou forma alcançou o que foi inicialmente proposto: procurar um tema específico e pertinente ao currículo de Matemática da Educação Básica com impacto na prática didática em sala de aula, abordando o conteúdo de Funções por meio de tarefas que envolvam criptografia.

No desenvolvimento, apresentamos a criptografia inserida em um contexto histórico, mostrando sua importância para a humanidade, camuflando informações, ajudando nas tomadas de decisões, no princípio, infelizmente, inseridas em um ambiente de guerras e depois, na proteção de dados pessoais, financeiros de um cidadão, de uma instituição financeira ou mesmo governamental, ou seja, na segurança em comunicação e na transmissão de dados.

Buscamos ainda, neste trabalho, indicar para o professor a possibilidade de atividades instigantes para o ensino de funções, envolvidas em um contexto real, mostrando assim uma aplicação, valorizando o conhecimento matemático e explicitando conceitos matemáticos do Ensino Fundamental e Médio.

Consideramos que o relato apresentado no capítulo 4, mostra que é possível envolver os alunos com o objeto de estudo, motivar e estimular a participação e aproveitar suas contribuições para o desenvolvimento passo a passo da aula. Enfatizando assim, a importância de dar uma aplicação ligada à sua realidade para assuntos desenvolvidos em sala, muitas vezes abstratos.

Proporcionar um ensino contextualizado significa propor uma educação diferenciada, nessa perspectiva, Silva (2007, p. 10) expressa que

> [...] a contextualização se apresenta como um modo de ensinar conceitos das ciências ligados à vivência dos alunos, seja ela pensada como recurso pedagógico ou como princípio norteador do processo de ensino. A contextualização como princípio norteador caracteriza-se pelas relações estabelecidas entre o que o aluno sabe sobre o contexto a ser estudado e os conteúdos específicos que servem de explicações e entendimento desse contexto [...].

De outro ponto de vista e reavaliando minha prática, posso afirmar terminantemente que a participação neste mestrado e na elaboração deste trabalho, contribuiu significativamente para uma mudança na minha prática, pois me trouxe reflexões que até então não me preocupava, principalmente em torno de planejamentos, prazos ou mesmo com relação a um olhar diferenciado ao entendimento deste aluno e as suas possíveis dificuldades apresentadas no conceito exposto.

Repensando e analisando a experiência vivenciada, pude perceber um cuidado maior na elaboração de tarefas, ou mesmo na associação das definições no olhar do aluno, investigando o porquê ele chegou naquela conclusão e, a partir desta construir uma estratégia para alcançar os objetivos propostos.

Assim, desejamos que este trabalho possa ajudar outros educadores e que venha contribuir e sensibilizar sobre a importância do ensino da matemática através da contextualização presente na vida do educando.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Jander Rocha. **Avaliação de desempenho dos Criptossistemas de Curvas Elípticas de Menezes- Vanstone e do Análogo de Elgamal no contexto de encriptação de imagens**. 2017. 49f. Monografia (Graduação – Curso de Ciência da Computação) – Universidade Federal do Maranhão, São Luís, 2017.

BAUMGART, John K. Álgebra. **Tópicos de História da Matemática para uso de sala de aula.** Tradução de Hygino Domingues, São Paulo: Atual Editora, 1992.

BEZERRA, Débora de Jesus; MALAGUTTI, Pedro Luiz e RODRIGUES, Vânia Cristina da Silva. **Aprendendo Criptologia de forma divertida**. V Bienal da SBM. UFPB: 2010.

BRASIL. Ministério de Educação e Cultura. LDB - Lei nº 9394/96, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da Educação Nacional. Brasília: MEC, 1996.

BRASIL. Secretaria da Educação Média e Tecnológica. Parâmetros Curriculares Nacionais/ Ensino Médio. Parte III – Ciências da Natureza, Matemática e suas Tecnologias. Brasília, 2000.

CARAÇA, Bento de Jesus. **Conceitos fundamentais da Matemática**. 9º ed. Lisboa: Sá da Costa,1989.

DANTAS, George Felipe de Lima. ***Esteganografia digital***, Brasília, ago. 2002. Disponível em: <https://blogandoseguranca.blogspot.com/2007/12/esteganografia-digital.html>. Acesso em: 8 jan. 2021.

EVES, Howard**.** ***Introdução à História da Matemática***. Tradução de Hygino Domingues. 5ª ed. – Campinas: Editora da Unicamp, 2011.

FERREIRA, Rosiney de Jesus. **Matemática e Arte um Diálogo Possível: Trabalhando Atividades Contextualizadas em Sala de Aula**. XI ENEM – Encontro Nacional de Educação Matemática. SBEM – Sociedade Brasileira de Educação Matemática. 2013.

FERREIRA, Rosiney de Jesus. **Matemática e Arte, Um Diálogo Possível: Trabalhando atividades interdisciplinares no 9° ano do ensino fundamental**. 2015. 133 f. Dissertação (mestrado profissional - Programa de Pós-graduação em Educação Matemática) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. 2015.

FILHO, Daniel Cordeiro de Morais; MALAGUTTI, Pedro Luiz Aparecido. ***Matemática discreta****:* módulo II. Cuiabá, MT: Central de Texto, 2013. – (Matem@tica na pr@tica. Curso de especialização em ensino de matemática para o ensino médio) – Universidade Aberta do Brasil. 2013.

IEZZI, Gelson; MURAKAMI, Carlos. ***Fundamentos de Matemática Elementar.*** Volume 1: conjuntos, funções. 7 ed. São Paulo. Atual. 1993.

JASCONE, Fábio Luis Tavares. ***Protótipo de Software para Ocultar Texto Criptografado em Imagens Digitais***. 2003. 64f. Trabalho de Conclusão de Curso – Ciências da Computação. Universidade Regional de Blumenau, Blumenau, 2003.

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

MACHADO, Geraldo Magela. ***História da Comunicação Humana****.* InfoEscola Navegando e Aprendendo. Disponível em: <*https://www.infoescola.com/historia/historia-da-comunicacao-humana/*>. Acesso em: 11, nov.2020.

MEDEIROS, Fábio. *Criptografia:* ***Bastão de Licurgo (scytale).*** 2013. Disponível em: < https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-empython/>. Acesso em: 27 nov. 2020.

MOURA, Moises de Oliveira. ***A Criptografia Motivando o Estudo das Funções no 9º Ano do Ensino Fundamental***. 2019. 92 f. Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Campus Universitário de Arraias - Curso de Pós-graduação (Mestrado) Profissional em Matemática, Arraias, TO, 2019.

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.

PETRI, M. ***Esteganografia***. Trabalho de conclusão de curso enviado ao Instituto Superior Tupy, Joinville, 2004.

PINTO, F. C. F.; DIAS, E. **Educação e Sociedade. Ensaio: Avaliação e Políticas Públicas em Educação**. Rio de Janeiro, v. 27, n. 104, p. 449-454, jun. 2019.

POPA, R. **An analysis of steganography techniques**. *Master's thesis, Department of Computer Science and Software Engineering of The "Polytechnic" University of Timisoara,* Timisoara, Romênia, 1998.

RAMOS, Maria Aparecida Roseane. ***TK006 – O Conceito de Função: de Leibniz a Riemann*****.** X SNHM – X Seminário Nacional de História da Matemática, 2013.

SANTOS, José Luiz dos. **A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica.** 2013. 81f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Universidade Federal da Bahia, Salvador, 2013.

SINGH, Simon. ***O livro dos Códigos***: A ciência do sigilo - do antigo Egito à Criptografia Quântica. Record, 12ª Edição. Rio de Janeiro. 2020.

SILVA, E. L. **Contextualização no ensino de química**: ideias e proposições de um grupo de professores. 2007. 143 f. Dissertação (Mestrado em Educação) – Faculdade de Educação, Universidade de São Paulo, São Paulo, 2007.

VICENTE, Aparecido; ARAÚJO, Bernardo de; ROCHA, Luciano Magno, ALMEIDA, Vitor Henrique Ferreira de Lima; HADDAD, Elias. **A CRIPTOGRAFIA E SUA IMPORTÂNCIA NA ATUALIDADE.** Revista Atena@. Vol. 1 – Número 1 – 2016.