INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA
E TECNOLOGIA DO AMAPÁ – IFAP
CAMPUS MACAPÁ

CURSO SUPERIOR DE LICENCIATURA EM MATEMÁTICA

LUCIANA DOS SANTOS RODRIGUES
SALOMÃO LIMA MONTEIRO

CRIPTODÁTICA:

criptografia como uma proposta didática para o estudo de funções afins e suas inversas

MACAPÁ – AP
2020

LUCIANA DOS SANTOS RODRIGUES
SALOMÃO LIMA MONTEIRO

CRIPTODÁTICA:

criptografia como uma proposta didática para o estudo de funções afins e suas inversas

Trabalho de Conclusão de Curso apresentado ao curso Superior de Licenciatura em Matemática, do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, campus Macapá, como requisito avaliativo para obtenção de título de Licenciandos em Matemática.
Orientador: Prof. Me. André Luiz dos Santos Ferreira.
Coorientador: Prof. Esp. Eonay Barbosa Gurjão.

MACAPÁ – AP
2020

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

R696c Rodrigues, Luciana dos Santos
CriptoDática: criptografia como uma proposta didática para o estudo de Funções Afins e suas Inversas / Luciana dos Santos Rodrigues, Salomão Lima Monteiro. - Macapá, 2020.
70 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Licenciatura em Matemática, 2020.

Orientador: Me. André Luiz dos Santos Ferreira.
Coorientador: Esp. Eonay Barbosa Gurjão.

1. Função Afim e sua Inversa. 2. Criptografia. 3. CriptoDática. I. Monteiro, Salomão Lima. I. Ferreira, Me. André Luiz dos Santos, orient. II. Gurjão, Esp. Eonay Barbosa, coorient. III. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

LUCIANA DOS SANTOS RODRIGUES
SALOMÃO LIMA MONTEIRO

CRIPTODÁTICA:

criptografia como uma proposta didática para o estudo de funções afins e suas inversas

Trabalho de Conclusão de Curso apresentado ao curso Superior de Licenciatura em Matemática, do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, campus Macapá, como requisito avaliativo para obtenção de título de Licenciandos em Matemática.
Orientador: Prof. Me. André Luiz dos Santos Ferreira.
Coorientador: Prof. Esp. Eonay Barbosa Gurjão.

BANCA EXAMINADORA

Prof. Me. André Luiz dos Santos Ferreira – Orientador.

Prof. Esp. Eonay Barbosa Gurjão – Coorientador.

Prof. Dr. Carlos Alexandre Santana Oliveira – Avaliador

Prof. Me. Romaro Antonio Silva – Avaliador

Prof. Esp. Danilo da silva Miranda – Avaliador

Aprovado em 07, de dezembro de 2020.

Dedico este trabalho com amor e reverência aos meus antepassados.

Aos meus familiares, sobretudo à minha avó Rossilda Furtado, responsável pela maior herança da minha vida: “meus estudos”.

Aos meus futuros filhos e descendentes, desejo que estudem com a firme certeza de que tudo que requer esforços e disciplina resulta em felicidade e grandes conquistas.

Luciana dos Santos Rodrigues.

Dedico este trabalho ao meu querido irmão, Deyvid Emanuel Lima Monteiro, incentivando-o a sempre prosseguir com os estudos.

Aos meus futuros filhos, quero dizer que já os amo.

Aos meus pais que juntamente comigo se sentem realizados com essa conquista.

***Salomão Lima Monteiro*.**

AGRADECIMENTOS

À Deus por ter criado tudo no Universo e a essência da Vida;

À minha mãe Josiane Furtado e meus irmãos, Wanessa Santos e Lucas Santos, por me apoiarem e compreenderem o meu isolamento em inúmeras vezes;

Ao meu companheiro Tayson Coutinho, pelo amor e dedicação para comigo;

Aos colegas da graduação pelos vários momentos de estudos e descontrações, em especial a Fabiola; Rosimara, Andressa, Bruna, Amanda e Ingredy, pela amizade e por serem mulheres de mente brilhante e criativa, ao Jovino, Salomão, Luiz e Alerrandresson que se tornaram mais que colegas, amigos, que fizeram essa jornada mais leve;

Ao professor André Ferreira, pela orientação, apoio e pelas sugestões apresentadas no decorrer desta jornada e ao professor Eonay Barbosa, pela coorientação e auxílio na construção do software CriptoDática;

Ao professor Romaro Silva, principalmente, pela disposição e paciência;

Ao Professor Dr. Carlos Alexandre e ao professor Esp. Danilo Miranda que aceitaram participar da banca de avaliação desta pesquisa;

Ao IFAP e a todos os professores que contribuíram com a minha trajetória acadêmica e pela elevada qualidade do ensino oferecido, agradeço especialmente ao professor Esp. Marcio Abreu, professor Dr. Jonatham Amanajás, professora Me. Shirly Santos e professora Dr. Veralúcia Severino, por me proporcionarem conhecimento não apenas racional, mas pelas valiosas contribuições dadas durante todo o processo da minha formação profissional.

Luciana dos Santos Rodrigues.

AGRADECIMENTOS

À Deus em primeiro lugar, que permitiu a conclusão desse trabalho;

Aos meus colegas de classe, pela caminhada acadêmicas e parceria, pelos debates construtivos e discussões temáticas;

Aos professores que nos instruíram;

Ao colega ANTONIO JOVINO SANTOS DA SILVA, que além de companheiro de curso se tornou um amigo excepcional;

Ao companheiro de curso EDIVALDO BASTOS DA SILVA pela parcerias em trabalhos acadêmicos;

Ao meu Orientador André Luiz dos santos Ferreira, que sempre se fez muito presente nessa caminhada, seja como PROFESSOR instruindo, AMIGO aconselhando, PAI cobrando e preocupando-se;

Ao meu co-orientador Eonay Barbosa Gurjão, por sempre está disposto a ajudar e dedicar seu tempo para apoiar um amigo, grato por apoiar essa ideia;

Ao meu amigo Gabriel de Oliveira Martins por sempre me incentivar, incentivo mútuo este que começou em 2014 quando nos reuníamos e estudávamos para o vestibular;

A toda a minha família que de alguma forma contribuíram e estiveram presente nessa jornada.

Salomão Lima Monteiro.

RESUMO

O presente trabalho envolve uma proposta de associar o tema Criptografia ao conteúdo de Funções, mais especificamente função Afim e sua Inversa, na qual, é apresentado o CriptoDática, um Software aplicativo desenvolvido pelos autores, que busca auxiliar nessa associação de forma mais prática e didática. A criptografia atualmente é uma essencial ferramenta no estudo de sistemas de construção de algoritmos matemáticos, ao ter fundamentos matemáticos, a criptografia baseia-se em princípios e técnicas ao codificar e decodificar mensagens que compreende um processo de fazer e desfazer algo, o que é similar ao princípio da função inversa. Associar o ensino de funções à criptografia é uma forma de informar ao discente de que tudo aquilo que ele estudou até então, por mais básico que seja, é aplicável e útil. Para a produção dos dados desta pesquisa, primeiro houve a apresentação do CriptoDádita, por meio de um vídeo tutorial, juntamente com a proposta didática, posteriormente, os pesquisados foram convidados a responder um questionário através de uma plataforma digital online, *Google forms*, organizada em treze questões e dividida por dois eixos, o primeiro eixo é sobre o perfil dos professores, o segundo eixo é sobre a avaliação feita do aplicativo CriptoDática, através da experiencia e seu fazer pedagógico para uma a análise que converge para um conhecimento necessário em relação a compreensão dessa ferramenta proposta. Como um resultado, a proposta da ferramenta CriptoDática apresentou ser aceitável, visto que os professores pesquisados consideraram útil, uma vez que a utilização do CripitoDática, bem como, com as devidas adaptações e correções futuras, possa potencializar a associação do estudo da criptografia com funções afins e suas inversas. E futuramente como extensões deste trabalho, podem ser realizadas pesquisas de campo em sala de aula para que alunos e professores avaliem a utilização deste objeto de aprendizagem nas atividades de ensino-aprendizagem, bem como, podem ser elaboradas novas versões e outros objetos de aprendizagem com novos temas voltados a criptografia para atingir novos públicos.

Palavras-Chave: CriptoDática. Função Afim e suas Inversas. Criptografia.

ABSTRACT

The present work involves a proposal of associating the Cryptography theme to the Content of Functions, more specifically the Like function and its Inverse, in which CriptoDática is presented, an application Software developed by the authors, which seeks to assist in this association in a more practical and didactic way. Cryptography is currently an essential tool in the study of systems for building mathematical algorithms, having mathematical foundations, cryptography is based on principles and techniques when encoding and decoding messages that comprise a process of doing and undoing something, which is similar to the principle of the inverse function. Associating the teaching of functions with cryptography is a way to inform the student that everything he has studied so far, however basic, is applicable and useful. To produce the data of this survey, first there was the presentation of CriptoDática through a video tutorial along with the didactic proposal, later, the respondents were invited to answer a questionnaire through an online digital platform, Google forms, organized in thirteen questions and divided by two axes, the first axis is about the profile of teachers, the second axis is about the evaluation made of the CriptoDática application, through the experience and its pedagogical making for an analysis that converges to a necessary knowledge in relation to understanding this proposed tool. As a result, the CriptoDática tool proposal was acceptable, since the surveyed teachers considered it useful, since the use of CriptoDática, as well as, with the necessary adaptations and corrections in the future, could potentialize the association of the cryptology study with related functions and its inverse. And in the future, as extensions of this work, field research can be carried out in the classroom for students and teachers to evaluate the use of this learning object in teaching-learning activities, as well as new versions and other learning objects with new themes focused on cryptography to reach new audiences.

Keywords: CriptoDática. Related Function and its Inverse. Cryptography.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

BNCC	Base Nacional Comum Curricular.
COVID-19	Doença do Corona Vírus.
CPF	Certificado De Pessoa Física.
CSS	*Cascading Style Sheets.*
DES	*Data Encryption Standard*
E2EE	*end to end encryption.*
HTML	*Hypertext Markup Language.*
JS	*JavaScript.*
ONSEN Ui 2.0	*open-source UI*
PCN	Parâmetros Curriculares Nacionais
PHP	*Hypertext Preprocessor*
PWAs	*Progressive Web Apps* (PWAs)
RG	Registro Gera.
RSA	*Rivest Shamir Adleman.*
TDIC	Tecnologias Digitais de Informação e Comunicação
TSE	Tribunal Superior Eleitoral.

SUMÁRIO

1 INTRODUÇÃO

A criptografia é a ciência que estuda métodos para codificar mensagens de maneira segura, de forma que, apenas seu destinatário consiga interpretá-la. E para as mídias digitais, ela serve como uma forma de preservar a privacidade, ao ocultar algumas informações como senhas, transações bancárias entre outros, Segundo Ludwig, Rebelatto e Silva (2020, p. 46), "A criptografia tem como princípio permitir a comunicação entre um remetente e um destinatário de modo que terceiros não tenham acesso ao conteúdo compartilhado". Isto é, a comunicação digital requer deste anteparo para garantir o sigilo necessário na comunicação.

Temas atuais, de preferência tecnológicos, quase sempre chamam a atenção dos alunos, acompanhar essa evolução e reciclar esses temas reorganizando-os de um ponto de vista didático e aplicados à educação, o tema tecnológico torna-se uma excelente estratégia pedagógica, segundo Medeiros (2020):

> O ensino de matemática ao ser relacionado com o cotidiano do aluno e com outras ciências torna-se mais prazeroso, produtivo e significativo, pois o aluno pode ver a importância de um determinado conhecimento não apenas dentro da própria disciplina, mas em outras áreas do saber, e isso dá mais sentido ao estudo realizado. (MEDEIROS, 2020, p. 16)

É nessa perspectiva de contextualização**,** que o presente estudo faz a associação do tema de criptografia ao conteúdo de funções, mais especificamente função Afim e sua Inversa como proposta didática. E para auxiliar o professor de matemática com essa proposta em seu trabalho de sala de aula, foi desenvolvido um software com o intuito de dinamizar, estimular e dar variabilidade na utilização de questões propostas relacionadas a criptografia e inversão de funções, no sentido de tornar os aspectos do conteúdo de funções mais compreensíveis ao entendimento dos alunos através dessa associação e interatividade com novas ferramentas e metodologias.

Utilizar temas atuais e métodos dinâmicos no processo de ensino e aprendizagem na matemática, é mencionado nos Parâmetros Curriculares Nacionais de matemática (1997), como:

> A vitalidade da matemática deve-se também ao fato de que, apesar de seu caráter abstrato, seus conceitos e resultados têm origem no mundo real e encontram muitas aplicações em outras ciências e em inúmeros aspectos práticos da vida diária. (BRASIL, 1997, p. 23)

Logo, a criptografia torna-se um motivador de enorme potencial a ser explorado na matemática, tanto para contextualizar diversos assuntos, quanto para a aplicação de várias definições. Por exemplo, a ideia de bijetividade estudada na definição de função bijetora, que é uma correspondência biunívoca entre dois conjuntos A e B, sendo que A se relaciona com B, de forma biunívoca, para cada elemento de A existe um único corresponde em B, isso permite a volta de B para A, quando uma função é bijetora ela pode admitir uma inversa conhecida como função inversa e o método de codificar e decodificar só fará sentido se a função escolhida for bijetora, em outras palavras, se a função escolhida for invertível, e esta característica da invertibilidade, é a garantia necessária para os receptores revelarem as informações codificadas.

Buscando desenvolver o estudo, chegou-se aos seguinte problema: Como dinamizar, estimular e dar variabilidade na aplicação de questões propostas relacionadas a criptografia e inversão de funções através do uso de um software?

Para responder tais questões, traçou-se o seguinte objetivo geral: utilizar a criptografia para relacionar teoria e prática, estabelecendo relações entre o desembaralhar de um código e as Funções Inversas, na perspectiva da utilidade da matemática envolvida em seu funcionamento. Para tanto, foram traçados os seguintes objetivos específicos: Produzir um ensino interativo sobre Funções Afins e Inversas e tornar as aulas mais dinâmicas; Utilizar a Criptografia como tema gerador para o estudo das funções Afins e suas Inversas; Desenvolver um software aplicativo (CriptoDática) para relacionar o tema criptografia com o estudo de funções Afins e suas inversas facilitando a aplicação em sala de aula; Mostrar a aplicação de Funções Afins na criação de cifras de substituição através da ferramenta CriptoDática.

Assim, será testado e discutido a eficácia do CriptoDática e da temática utilizada em relação ao aprendizado dos conceitos teóricos.

Nos capítulos seguintes apresentamos o conceito de criptografia e o resumo dos principais aspectos históricos, bem como, as definições dos conceitos básicos de funções, que é a base para o desenvolvimento do trabalho e em seguida a metodologia proposta.

Com base em uma consulta feita a professores do ensino básico do estado do amapá, acerca da metodologia proposta utilizando a criptografia como tema motivador e um software aplicativo como ferramenta para o ensino de funções inversas, foi possível fazer a tabulação a partir da opinião dos professores em relação a aplicação quanto a sua relevância para o ensino de funções Afins e suas inversas.

Desta forma, com base na avaliação dos professores e com as devidas adaptações e correções futuras poderemos adequar a proposta assim como o aplicativo com intuito de fundamentar a continuação deste trabalho sob outras perspectivas.

2 CRIPTOGRAFIA

A palavra Criptografia surgiu do Grego *Cryptos* que significa escondido e grafia *gráphein* que significa escrita, a criptografia também é a arte ou a ciência para se escrever cifras ou códigos por meio de recursos matemáticos, assim, apenas quem possui as chaves de decodificação das mensagens poderá interpretá-los. (SÁ, 2018)

2.2 Principais aspectos históricos da criptografia

A ideia de proteger informações é muito antiga, sejam elas segredos familiares, segredos religiosos, segredos militares ou governamentais. Segundo Singh (2014):

> Durante milhares de anos reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos, ao mesmo tempo todos estavam cientes das consequências de suas informações caírem em mãos erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para forças inimigas. (SINGH, 2014, p.11)

A busca pelo sigilo dessas informações preciosas, levou as nações a desenvolverem métodos de comunicações de segurança através de códigos, ocasionando a criação de mecanismos capazes de assegurar que dados sigilosos não fossem interceptados por inimigos e nem pelos seus mensageiros, a partir dessa necessidade foi criado uma das primeiras formas de criptografia, os chamados Métodos de Substituição.

A criptografia pode ser dividida em duas áreas e classificadas como: transposição e substituição. Na transposição, segundo Singh (2014, p. 23), “[...], as letras da mensagem são simplesmente rearranjadas, gerando, efetivamente um anagrama”. Isto é, as letras mantêm sua identidade alterando apenas sua posição.

Quanto ao ramo da substituição, surgiu como alternativa para o ramo da transposição. Trata-se da substituição de cada letra no texto por uma letra diferente de modo a complementar a cifra de transposição, isto é, cada letra conserva sua posição, porém, é substituída por uma outra letra ou símbolo. (SANTOS, 2016)

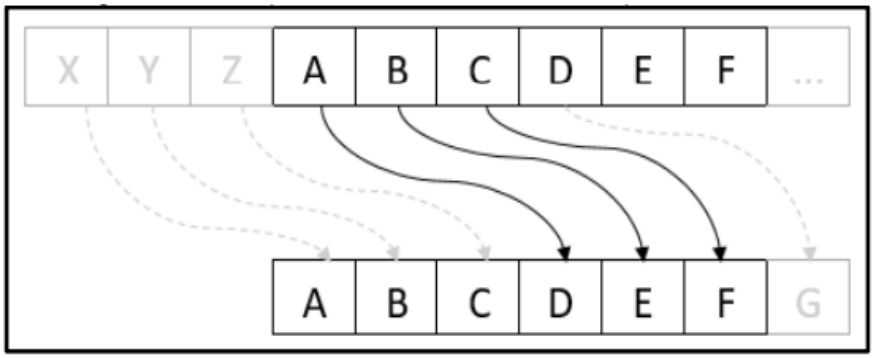
2.1.1 Cifra de Júlio César

Sabe-se que o primeiro registro de utilização de cifra por substituição foi desenvolvido pelo imperador romano Júlio César (100 a.C. – 44 a.C.), para troca de mensagens militares durante seu governo.

Estes registros são encontrados nos documentos que narram a Guerra de Gália do século I a.C., neste registro, César descreve como mandou uma mensagem para Cícero, informando que substituiu as letras do alfabeto romano por letras gregas, Cesar, às vezes, substituía cada letra da mensagem por outra que estivesse três casas à frente do mesmo alfabeto, este método de criptografia ficou conhecido como a "Cifra de César". (SINGH 2014).

A figura 1, ilustra como ocorre o deslocamento utilizado por César.

Figura 1 – Deslocamento utilizado por Júlio César.



Fonte**:** Dos autores, (2020).

Códigos como o de César padecem de um grande problema, são muito "fáceis de quebrar", ou seja, de ler a mensagem secreta mesmo não sendo o destinatário legítimo. Generalizando este raciocínio, podemos afirmar que qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto ocorre porque a frequência média com que cada letra aparece em um texto de uma determinada língua é mais ou menos constante. Por exemplo a frequência média de cada letra da língua portuguesa é dado conforme a tabela a seguir.

Tabela 1 – Frequência das letras no português.

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

Fonte: S. C. Coutinho, (2014).

Observe, entretanto, que este método para quebrar o código só funciona bem se a mensagem for longa. É fácil escrever uma mensagem curta, cuja contagem de frequência seja totalmente diferente da contagem de frequência média da língua portuguesa. Por exemplo, em "zuca zoou Zezé" a letra mais frequente é "Z", que aparece 4 vezes em um texto de 12 letras. Como 4/12 = 0,33, a porcentagem da letra "Z" no texto é de 33%; muito acima dos usuais da letra "Z" na frequência das letras no português que é 0,47%. Já a letra "A" aparece uma só vez, o que dá uma porcentagem de cerca de 8%; portanto, abaixo dos 14,64% usuais (COUTINHO, 2014).

A partir da cifra de César muitas outras cifras para a troca de mensagens militares originaram como a Cifra de Vigenére considerada uma evolução da Cifra de César, Cifra ADFGVX, Cifra do Chiqueiro, Cifra Lúcifer entre outros (SINGH, 2014).

2.1.2 Enigma

A máquina de cifras alemã Enigma pode ser considerada como sendo a mais promissora e desafiadora de toda a evolução da criptografia, como também a máquina de cifras mais conhecida no mundo, usada principalmente pelos alemães nazistas durante a Segunda Guerra Mundial, e o modelo utilizado por eles era conhecida como *Wehrmacht Enigma* (*Reichswehr* enigma D *Enigma-I*). De fato, Enigma é a marca de uma série de máquinas de criptografia, desenvolvidas antes e durante a Segunda Guerra Mundial, algumas das quais são compatíveis umas com as outras, e outras não (SINGH, 2014).

O mecanismo da Enigma segundo Rosseto (2018) consiste em:

> […] um teclado com 26 letras e um conjunto três de rotores dispostos em fila, além de um mecanismo de avanço que faz andar alguns rotores uma posição quando uma tecla é pressionada. Os alemães acrescentaram ainda um quarto rotor, chamado "refletor", assim, nenhuma letra da mensagem seria cifrada nela mesma. Também acrescentaram um dispositivo chamado stecker, que garantia a troca de pares de letras

> por outras sem importar qual unidade fosse usada para o processo. Com todo esse aperfeiçoamento, a máquina atingiu um total de 150 000 000 000 000 000 000 de combinações. (ROSSETO, 2018, p. 22)

O matemático e criptoanalista britânico Alan Turing e sua equipe decifraram com êxito as mensagens produzidas pela Enigma, eles trabalhavam no processo de decifração de códigos alemães durante a Segunda Guerra Mundial em *Bletchley Park*, também conhecida como *Station X* que era uma instalação militar secreta no Reino Unido.

Para auxiliar na interceptação e descodificação das mensagens dos alemães nazistas, Alan Turing desenvolveu uma máquina protótipo, originando o primeiro computador operacional para as atividades da inteligência britânico chamado de *Colossus*,.de acordo com Jesus (2013):

> Era um gigantesco computador, projetado especialmente para decifrar mensagens cifradas pela máquina enigma, que utilizava tecnologia de relés, e que podia ler 5.000 letras por segundo, através de um sistema fotoelétrico, e todas as possíveis combinações de mensagens codificadas eram comparadas com as mensagens geradas pelas chaves criptográficas do Colossus, para revelar a configuração da máquina usada pelos alemães. (JESUS, 2013, p. 19)

Assim começou a era moderna da criptografia, na qual o processo de programação de computadores começava a usar chaves de codificação muito mais complexas do que as utilizadas pela Enigma.

2.2 Criptografia na atualidade

Hoje, na era da comunicação, as informações codificadas e as tecnologias empregadas para produzi-las estão muito próximas do sujeito comum. Cada vez mais, são enviadas informações via web, compras realizadas on-line, cadastro de informações pessoais, como CPF e RG, ou até mesmo uma transação bancária via *Internet Banking*. Atualmente quem é responsável por garantir que nenhum terceiro fique sabendo dessas informações é a criptografia (FIGUEIREDO, 2010).

A criptografia atualmente é usada como uma técnica de troca de dados, como um código, ou algoritmo, para que eles se tornem indecifráveis, a não ser para quem possui a chave do código, ela consiste em dois principais tipos: a simétrica e a assimétrica.

Na criptografia simétrica, trata-se de uma chave simples, o algoritmo e a chave são idênticos, quer dizer, que o remetente e o destinatário usam chaves iguais. Pimenta (2004, p. 3)

afirma que, “Os algoritmos mais utilizados na criptografia de chave simétrica são o DES e o IDEA”.

Quanto a assimétrica, utiliza-se duas chaves que estão relacionadas matematicamente, uma chave denomina-se Chave Pública para criptografar, na qual, é aberta para que todos possam ver, e a outra chave denomina-se Chave Privada para descriptografar que é mantida em sigilo. Pimenta (2004, p. 3) afirma que, “Os algoritmos mais utilizados na criptografia assimétrica é o RSA e o Diffie-Hellman”. Portanto, as mensagens criptografadas com a chave pública só podem ser descriptografadas com a chave privada correspondente do destinatário.

2.2.1 Assinatura digital

A Assinatura Digital, é outra ferramenta que atualmente é utilizada para garantir a integridade de dados ou documentos e utiliza de criptografia assimétrica para sua execução. É importante ressaltar que a assinatura digital não deve ser confundida com a imagem digitalizada de uma assinatura manual e nem mesmo com certificado digital (RESENDE, 2009). Sobre a assinatura digital Marcacini (2002) diz:

> É, na verdade, uma sequência de bits que foi gerada mediante uma função matemática unidirecional aplicada ao documento, com o uso de uma chave privada que é única e exclusiva do usuário. A sequência de bits que forma a assinatura digital só poderia ter sido gerada por aquele que detém a chave privada, o que permite atribuir-lhe a mesma exclusividade da assinatura manuscrita. (MARCACINI, 2002 p. 185)

No momento em que é criado uma assinatura digital, ela é associada a um documento, e esta assinatura digital só será autêntica para tal documento, ou seja, para cada documento há uma assinatura distinta, até mesmo se for da mesma pessoa.

As urnas eletrônicas, também utilizam a criptografia em seu hardware e software por meio da assinatura digital. Segundo a Tribunal Superior Eleitoral – TSE (2020), afirma que:

> A urna eletrônica utiliza o que há de mais moderno quanto às tecnologias de criptografia, assinatura digital e resumo digital. Toda essa tecnologia é utilizada pelo hardware e pelo software da urna eletrônica para criar uma cadeia de confiança, garantindo que somente o software desenvolvido pelo TSE, gerado durante a cerimônia de lacração dos sistemas eleitorais, pode ser executado nas urnas eletrônicas devidamente certificadas pela Justiça Eleitoral. (BRASIL, 2020)

Utilizando de criptografia simétrica e assimétrica para sua execução de seus algoritmos que são de conhecimento exclusivo do Tribunal Superior Eleitoral (BRASIL, 2020).

2.2.2 Criptografia de Ponta a Ponta (*end to end encryption* – E2EE*)*

Para Teixeira *et al* (2017, p. 608), “A sociedade da informação é uma realidade irreversível, pois a inserção da tecnologia no cotidiano das pessoas cada vez mais gera um intervalo mínimo entre a sensação de uma novidade e o que, em seguida, vem a se tornar uma necessidade”. Os aplicativos gratuitos de troca de mensagens se enquadram nesta circunstância pois utilizam a simples conexão à internet para atividades essenciais humanas e/ou corporativas, porque viabiliza uma comunicação de alta velocidade e sem custos financeiros.

A simplicidade de troca de mensagens por meio de aplicativos demanda certa segurança para garantir um mínimo de privacidade, Teixeira *et al* (2017, p. 608), “Empresas do ramo de tecnologia de informação têm buscado técnicas protetivas para tanto, tal como o uso da criptografia em sistemas operacionais e aplicativos”. Com intuito de garantir maior proteção aos usuários essas empresas lançaram o sistema de criptografia de ponto a ponto em ingles *end to end* ou E2EE, e utiliza de criptografia assimétrica para sua execução.

A criptografia de ponta a ponta é usada atualmente por aplicativos de troca de mensagens populares como o *WhatsApp* e *Telegram*, os sistemas criam chaves criptográficas públicas e privadas para cada pessoa que adere.

A segurança por trás da criptografia “ponta a ponta” é ativada pela criação de um par de chaves pública-privada. Esse processo, também conhecido como criptografia assimétrica, que emprega chaves criptográficas separadas para proteger e descriptografar a mensagem. As chaves públicas são amplamente divulgadas e usadas para bloquear ou criptografar uma mensagem. As chaves privadas são conhecidas apenas pelo proprietário e são usadas para desbloquear ou descriptografar a mensagem. As vantagens da criptografia de ponta a ponta podem ser resumidas da seguinte forma: Garante que seus dados estejam protegidos contra *hacks*; protege sua privacidade e protege os administradores (MACHADO e DONEDA, 2019).

3 FUNÇÕES

O conceito de funções é imprescindível para o desenvolvimento dos objetivos deste estudo e neste tópico serão apresentados os conceitos básicos sobre o estudo de Funções, função Afim e suas caracterizações, tais como: Função Injetora; Função Sobrejetora e Função Bijetora e assim que apresentados essas caracterizações serão a apresentados as noções de funções inversas.

O estudo de funções tem destaques em vários de seus ramos e claramente em outras áreas do conhecimento. Muitos fenômenos científicos como físicos, biológicos, sociais etc., apresentam seus feitos por meio das funções (ÁVILA, 2012; SILVA e ALEXANDRE 2014).

O conceito de função surge da consideração de grandezas variáveis que estão relacionadas entre si. Por variáveis, entendemos um símbolo que serve para denotar qualquer dos elementos de um dado conjunto, chamado o domínio da variável (ÁVILA, 2012).

Quanto a sua definição, chama-se toda correspondência f que atribui a cada valor de uma variável x em seu domínio (também chamado de domínio da função) um e um só valor de uma variável y num certo conjunto Y (também chamado de contradomínio da função), x é chamada de variável independente e y a variável dependente (ÁVILA, 2012).

Por exemplo: um automóvel viaja a $80\ Km/h$ percorre uma distância s (espaço) em t horas. Podemos, pois escrever: $s = 80t$. atribuindo a t valores arbitrários, calculamos o espaço percorrido s. Assim:

$$t = 2 \Rightarrow s = 80 \times 2 = 160;$$
$$t = 3 \Rightarrow s = 80 \times 3 = 240;$$
$$t = 1{,}5 \Rightarrow s = 80 \times 1{,}5 = 120;$$
$$t = 1{,}25 \Rightarrow s = 80 \times 1{,}25 = 100$$
$$\dots$$
$$\vdots$$
$$\dots$$

e assim por diante. Como se vê nesse exemplo há duas grandezas variáveis o espaço s e o tempo t. Ao tempo t atribuímos valores arbitrários e calculamos os valores correspondentes de s. É por isso que se diz que t é uma variável independente, enquanto s dependem dos valores atribuídos a t; esta dependência de s sobre t também se exprime dizendo que s é a função de t.

Quanto a notação de função costuma-se escrever, segunda Ávila (2012):

> $y = f(x)$ para indicar que y é uma função de x, e que lemos "y é igual a f de x". quando lidamos com várias funções ao mesmo tempo, usamos diferentes letras para distingui-las: $f(x)$; $g(x), h(x)$ e etc. A rigor, $f(x)$ é o valor da função no ponto x ou imagem x, sendo mais correto dizer "seja a função de x", embora frequentemente, se prefira essa última maneira de falar. Outro modo de indicar uma função consiste em escrever $f: x \mapsto f(x)$, que se lê: "f leva x em $f(x)$" (ÁVILA, 2012, p. 28).

Mas, para caracterizar uma função não basta dar a lei que a cada x faz corresponder um y; é preciso deixar claro qual é o domínio da função. Por isso a notação de função torna-se mais completa quando nela incluímos o domínio da função. Assim uma função genérica f com domínio D é denotada por $f: x \in D \mapsto f(x)$. Notação esta que deixa claro que cada x no domínio D é levado em $f(x)$, que é a imagem de x pela f (ÁVILA, 2012).

3.1 Caracterização das Funções

Uma função pode ser definida de várias formas, dependendo de como o seu conjunto domínio se relaciona com o conjunto do contradomínio. Ou seja, dependendo de como a função f mapeia valores reais em valores reais, podemos caracterizá-la em três tipos: Função Injetora, Função Sobrejetora e Função Bijetora.

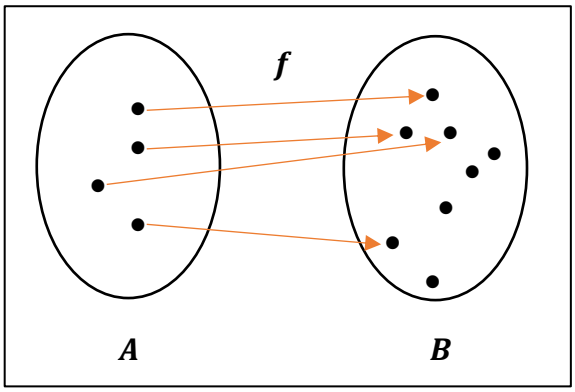
3.1.1 Função Injetora

A função injetora (ou injetiva), trata-se dos elementos de um conjunto domínio de uma função qualquer, se relacionando com elementos distintos do contradomínio dessa função.

Pode-se definir uma função injetora da seguinte forma: Sejam A e B o domínio e o contradomínio, respectivamente, de uma função f. Então f é injetora quando: $x1 \neq x2$ em $A \Rightarrow f(x1) \neq f(x2)$ em B, esses valores que pertencem ao contradomínio que fazem parte da função que compõe a imagem. Isto é, quando elementos diferentes de A são transformados por f em elementos diferentes de B, denominam-se Função Injetora ou Injetiva. (JANOS, 2009; VILANUEVA, 2014).

A figura 2, mostra uma função injetiva $f: A \to B$, com todos os elementos do conjunto A com um único correspondente no conjunto B.

Figura 2 – Função Injetora representada por diagramas de flexas.



Fonte**:** Dos autores, (2020).

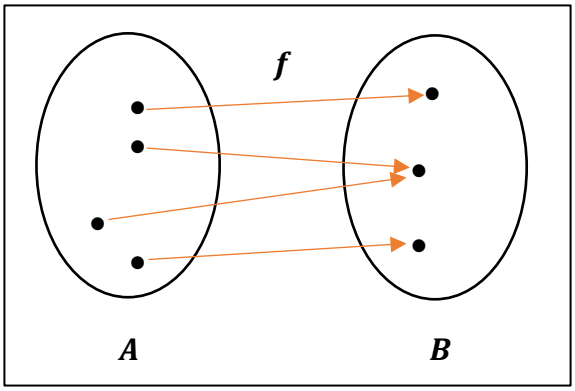
3.1.2 Função Sobrejetora

A função sobrejetora ou sobrejetiva é uma classificação de função matemática que relaciona elementos do domínio de uma função com suas respectivas imagens de forma que a imagem seja igual ao contradomínio.

Em notação uma função sobrejetora é dita como $f: A \rightarrow B$, para todo y pertencente ao conjunto B, encontra-se um x pertencente ao conjunto A que se relaciona com ele. Neste caso, temos que a imagem de f igual ao conjunto B (JANOS, 2009; VILANUEVA, 2014).

A figura 3, mostra uma função sobrejetiva, na qual, todos os elementos do conjunto B são correspondentes de pelo menos um elemento do conjunto A.

Figura 3 – Função sobrejetora representada por diagramas de flexas.



Fonte**:** Dos autores, (2020).

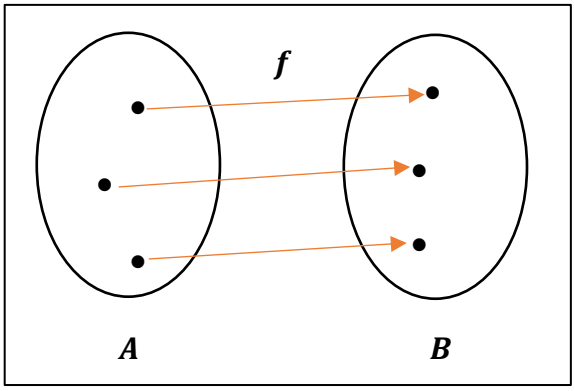
3.1.3 Função Bijetora

A Função Bijetora, trata-se da função que possui ao mesmo tempo duas propriedades ser Injetora e ser Sobrejetora. Isto é, uma função $f: A \rightarrow B$ é bijetora se e somente se, ela for

coincidentemente, injetora e sobrejetora, ou seja, quando há essa simultaneidade biunívoca entre os conjuntos domínio A e contradomínio B denominando-se Bijeção. Quando uma função é bijetora, ela pode admitir uma inversa conhecida como função inversa. (JANOS, 2009; VILANUEVA, 2014).

A figura 4, mostra uma função bijetora, onde todos os elementos do conjunto A tem um único correspondente em B e concomitantemente todos os elementos de B tem um único correspondente em A.

Figura 4 – Função bijetora representada por diagramas de flexas.



Fonte: Dos autores, (2020).

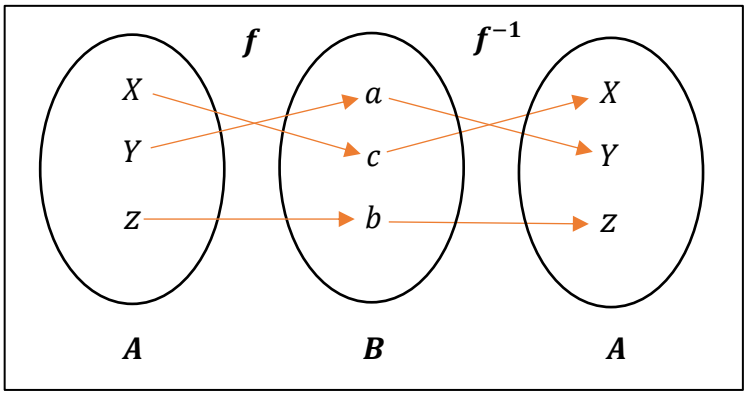
3.1.4 Função Inversa

No estudo da função Inversa é necessário conhecer as propriedades da função, ditas na sessão anterior, por exemplo que uma função bijetora pode admitir uma inversa conhecida como Função Inversa.

A função Inversa é obtida substituindo o domínio pela imagem da função. Deste modo, a inversa de uma função qualquer modifica o domínio e a imagem, ou seja, o domínio transforma-se em imagem e a imagem transforma-se em o domínio. Em termos informais, se f é uma função $A \rightarrow B$, então a função inversa de f, denotada por f^{-1}, é uma função $B \rightarrow A$. (JANOS, 2009; VILANUEVA, 2014).

Ou seja, se uma entrada x de A produz uma saída c de B em f^{-1} produzimos a saída x, como mostra na figura 5.

Figura 5 – Função Inversa representada por diagramas de flexas.



Fonte: Dos autores, (2020).

A inversa de uma função f, denota-se por f^{-1}, é a função que desfaz a operação executada pela função f.

3.2 Função Afim

Existem vários tipos de funções na matemática. E neste estudo vamos abordar, de uma forma curta e objetiva, a Função Afim.

A função Afim, também conhecida como função polinomial do primeiro grau, e é dada como uma função polinomial em que seu maior expoente é o número 1, e o gráfico dessa função é uma reta.

A função Afim pode ser definida como: uma função representada por $f: \mathbb{R} \to \mathbb{R}$, definida como $f(x) = ax + b$, sendo a e b números reais e $a \neq 0$ (JANOS, 2009; VILANUEVA, 2014).

Neste tipo de função, o número a é chamado de coeficiente de x, que representa a taxa de crescimento ou taxa de variação da função. Já o número b é chamado de termo constante.

As funções $f(x) = x + 5$, $g(x) = 3\sqrt{3x} - 8$ e $h(x) = 1/2\, x$, são exemplos de funções afim.

3.3 Criptografia e o ensino de Funções

Sobre o tema Criptografia no ensino básico, Pereira, (2015) afirma que:

> Muitos conceitos matemáticos utilizados em Criptografia fazem parte da grade curricular do Ensino de Matemática. Dessa forma, associar os conceitos a uma

> aplicação tão corrente nos dias de hoje, torna a aprendizagem mais significativa (PEREIRA, 2015, p. 6)

Alguns desses conceitos matemáticos utilizados na Criptografia são os de funções, especialmente os de funções invertíveis visto que ao criptografar e descriptografar estamos aplicando uma relação biunívoca entre a mensagem a ser enviada e o código a ser decodificado pelo receptor. Rosseto (2018, p. 30), ressalta que está associação fundamenta-se da seguinte maneira, "O método consiste em pegar uma informação e convertê-la em números através de uma função bijetiva e, pela aplicação de sua inversa transformar esses números novamente na informação original."

Segundo os PCNs (1997, p. 41) "Essas aprendizagens só serão possíveis na medida em que o professor proporcionar um ambiente de trabalho que estimule o aluno a criar, comparar, discutir, rever, perguntar e ampliar ideia."

Quando se fala em uma correspondência biunívoca, trata-se de dois conjuntos A e B, sendo que A se relaciona-se com B, de forma um a um, para cada elemento de A existe um único corresponde em B, isso permite a volta de B para A, isto é, quando uma função é bijetora, ela pode admitir uma inversa conhecida como função inversa e o método de codificar e decodificar precisa dessa característica de invertibilidade, para assim o receptor ser capaz de transformar a informação codificada na informação original, sem ambiguidade ou falta de informação (ROSSETO, 2018).

Para operar utilizando esta associação do tema de criptografia e assunto de funções, deve-se utilizar a função Afim $f(x) = ax + b$, com $a, b \in \mathbb{R}\ e\ a \neq 0$, pois esta função é sempre bijetiva sobre sua imagem e consequentemente admite inversa sobre sua imagem.

O processo de criptografia dar-se-á seguindo no mínimo 3 etapas, sendo as primeiras um processo de associação de símbolos (números) as letras, para posterior substituição em um texto embaralhados a partir de uma lei de formação (função). dCom esse objetivo deve-se seguir os passos, são eles: pré-criptografar a mensagem, criptografar a mensagem e descriptografar a mensagem.

O Motivo de pré criptografar a mensagem, é simplesmente para associar números as letras do alfabeto, pois como o intuito é criptografar mensagens usando funções, e elas operam somente com números, é preciso que os números aparecem de alguma forma, e a forma mais lógica é associar cada letra do alfabeto a um número como é mostrado na tabela 2.

Tabela 2 – Pré criptografia.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**ESPAÇO**
11	12	13	14	15	16	17	18	19	20	21	22	23	
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**Y**	**X**	**Z**	99
24	25	26	27	28	29	30	31	32	33	34	35	36	

Fonte: Dos autores, (2020).

No entanto para evitar ambiguidades, Rodrigues (2013), afirma que:

> Deve-se ressaltar que há várias possibilidades para se formar a relação entre letras e números, porém a mais indicada é que todas as letras sejam representadas por dois dígitos para se evitar duplo sentido, pois se começássemos essa relação a partir do número 1, com $A = 1$ e $B = 2$, e assim por diante, o número 11 poderia significar AA, ou ainda a letra K que é a 11ª letra do alfabeto. (RODRIGUES, 2013, p. 17)

Após associar cada letra do alfabeto a um número o passo seguinte é determinar uma mensagem a ser codificada e obter a sequência numérica correspondente ao texto de acordo com a tabela. Por exemplo a mensagem a ser criptografada pode ser: TESTANDO O CÓDIGO, a correspondência das letras é apresentada na tabela 3 a seguir.

Tabela 3 – Relação de cada letra da mensagem com seu respectivo numeral.

T	**E**	**S**	**T**	**A**	**N**	**D**	**O**	**ESPAÇO**	**O**	**ESPAÇO**	**C**	**O**	**D**	**I**	**G**	**O**
30	15	29	30	11	24	14	25	99	25	99	13	25	14	19	17	25

Fonte: Dos autores, (2020).

Após este momento, deve-se escolher uma função $f(x) = ax + b$, que receberá o valor da letra que deseja transmitir e gerar outro valor através da função escolhida. Supondo que $f(x) = ax + b$ seja a função $f(x) = 2x + 1$, esta será a função que fará o embaralhamento das letras da mensagem a ser criptografada que é: TESTANDO O CÓDIGO. Assim substituindo cada número da função cifradora:

$$T = 30, logo\ f(30) = 2\,.\,(30) + 1 = 61;$$
$$E = 15, logo\ f(15) = 2\,.\,(15) + 1 = 31;$$
$$S = 29, logo\ f(29) = 2\,.\,(29) + 1 = 59;$$
$$T = 30, logo\ f(30) = 2\,.\,(30) + 1 = 61;$$
$$A = 11, logo\ f(11) = 2\,.\,(11) + 1 = 23;$$
$$N = 24, logo\ f(24) = 2\,.\,(24) + 1 = 49;$$

$$\cdots$$
$$\vdots$$

...

$$espaço\ em\ branco = 99, logo\ f(99) = 2\,.\,(99) + 1 = 199;$$

e assim por diante, até a letra $O = 25, logo\ f(25) = 2\,.\,(25) + 1 = 51$.

A tabela 4, mostra a imagem da função, isto é, a sequência numérica encontrada da mensagem criptografada.

Tabela 4 – Mensagem criptografada.

T	**E**	**S**	**T**	**A**	**N**	**D**	**O**	**ESPAÇO**	**O**	**ESPAÇO**	**C**	**O**	**D**	**I**	**G**	**O**
61	31	59	61	23	49	29	51	199	51	199	27	51	29	39	35	51

Fonte: Dos autores, (2020).

Para decifrar uma mensagem o receptor calcula a imagem dos elementos, utilizando a função inversa, logo deve-se usar a inversa da função aplicada para criptografar, nesse caso é $f^{-1}(x) = \frac{(x-1)}{2}$. Restaurando a mensagem original:

$$f^{-1}(61) = \frac{(61-1)}{2} = 30;$$

$$f^{-1}(31) = \frac{(31-1)}{2} = 15;$$

$$f^{-1}(59) = \frac{(59-1)}{2} = 29;$$

$$f^{-1}(61) = \frac{(61-1)}{2} = 30;$$

$$f^{-1}(23) = \frac{(23-1)}{2} = 11;$$

$$f^{-1}(49) = \frac{(49-1)}{2} = 24;$$

$$espaço\ em\ branco: f^{-1}(199) = \frac{(199-1)}{2} = 99;$$

...
.
.
.
...

e assim por diante, até a o último algoritmo 51, logo $f^{-1}(51) = \frac{(51-1)}{2} = 25$.

Essa associação é uma atividade didática que é costumeiramente utilizada nos últimos anos do ensino fundamental e no Ensino Médio. Pereira (2015) diz:

> Podemos utilizar os conceitos de função aplicado à criptografia para ressaltar a relevância dos dois temas. Estabelecendo uma aplicação prática do conceito e assim tornando o ensino desse tema mais interessante. (PEREIRA, 2015, p. 54)

4 AS TDICs NO ENSINO BÁSICO

As tecnologias Digitais de Informação e Comunicação (TDIC's), referem-se a um conjunto de diferentes mídias que se diferenciam pela presença de tecnologia digital, isto é, são equipamentos que utilizam do processamento de dados armazenados e funcionam através de decodificação de códigos numéricos.

A contemporaneidade é fortemente marcada pelo desenvolvimento tecnológico digital e computacional, e alinhada a ao uso tecnológico como ferramenta pedagógica a Base Nacional Comum Curricular (2018), menciona as TDICs como:

> Tanto a computação quanto as tecnologias digitais de informação e comunicação (TDIC) estão cada vez mais presentes na vida de todos, não somente nos escritórios ou nas escolas, mas nos nossos bolsos, nas cozinhas, nos automóveis, nas roupas etc. Além disso, grande parte das informações produzidas pela humanidade está armazenada digitalmente. Isso denota o quanto o mundo produtivo e o cotidiano estão sendo movidos por tecnologias digitais, situação que tende a se acentuar fortemente no futuro. (BRASIL, 2018, p. 473)

Por efeito deste cenário, a escola por sua vez viu-se no dever de adaptar-se a esses novos elementos.

Em razão da nova rotina de estudo ocasionada pelo efeito da pandemia do novo Corona vírus (COVID-19), e a consequente implementação do isolamento social, medidas de confinamento e fechamento das escolas, exigindo que o ensino e aprendizagem aconteça quase que exclusivamente a distância, tornando rotineiro o uso de ferramentas digitais para os educadores e educandos como: *Meet; YouTube; Google classroom; WhatsApp; E-mails* e etc., e é justamente nesse ponto que as TDICs desempenham um importante papel.

Diante do desenvolvimento da sociedade e as responsabilidades com os impactos dessas transformações a Base Nacional Comum Curricular (BNCC) define dez competências gerais que devem ser desenvolvidas por todos os alunos na escola, e a quinta competência geral que é a competência "Cultura Digital", a BNCC (2018) fala:

> 5.Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva. (BRASIL, 2018, p. 9)

Essa competência fala da capacidade do estudante de compreender e utilizar tecnologias com ética, criticidade tanto para obterem informações como também produzirem e serem protagonistas do mundo.

A questão da tecnologia digital, não aparece somente na competência “Cultura Digital”, ela é mencionada igualmente na primeira e ne segunda competência geral da BNCC, denominadas de: “Conhecimento” e “Pensamento Científico, Crítico e Criativo”.

A competência “Conhecimento”, trata-se da utilização dos conhecimentos adquiridos sobre o mundo físico, social, cultural e digital na sua realidade. A Segunda competência que é o “Pensamento Científico, Crítico e Criativo”, nela os alunos irão investigar causas, elaborarem e testarem hipótese, trabalhar com a reflexão e resolução de problemas inclusive tecnológicas. (BRASIL, 2018)

O papel das TDICs no contexto escolar não é simplesmente ser um auxiliar, um suporte, mas sim apresentar novas possibilidades de desafios didáticos para o desenvolvimento de competências e de compreensão dos alunos, ou seja, despertar a pesquisa, a indagação, o lado criativo e investigativo, permitindo dessa forma a construção do conhecimento.

Tradicionalmente evidenciamos a utilização dos conhecimentos construídos sobre o mundo físico, social, cultural e digital para entender e esclarecer a realidade em que vivemos, acrescentando para a construção de uma sociedade justa, democrática e inclusiva, de acordo com as BNCC (2018, p.61), “[..] Os jovens têm se engajado cada vez mais como protagonistas da cultura digital, envolvendo-se diretamente em novas formas de interação multimidiática e multimodal e de atuação social em rede, que se realizam de modo cada vez mais ágil”. Quando se fala em cultura digital, não é necessariamente o estudante saber lidar com aparelhos eletrônicos, pois ao aproveitar o potencial de comunicação do universo digital, deve-se ficar atento com as interações do estudante com as TDICs, para a BNCC (2018):

> […], essa cultura também apresenta forte apelo emocional e induz ao imediatismo de respostas e à efemeridade das informações, privilegiando análises superficiais e o uso de imagens e formas de expressão mais sintéticas, diferentes dos modos de dizer e argumentar característicos da vida escolar. (BRASIL, 2018, p. 61)

A ideia de cultura digital é trabalhar o uso ético e responsável da tecnologia, em benefício de criar, inovar e produzir novas tecnologias, isto é, preparar o estudante para as TDICs.

4.1 As TDICs no ensino da matemática

As tecnologias Digitais de Informação e Comunicação (TDIC's) no ensino da matemática, têm como fundamental objetivo evidenciar a necessidade de novas práticas didático-metodológicas com o uso das mídias e tecnologias digitais nas escolas. (BUENO, BALLEJO, e VIALI 2020)

A área de matemática, que por muito tempo se caracterizou como ensino fechado, ganharam espaço com as TDICs, por exemplo, os softwares matemáticos muito úteis para explorar temas na área de matemática, são alguns: *Winplot;* Geogebra; *Poly; Modelus*; Cinderela; *Surfer; Morenamets; Scrath; Wolfram Alpha e* entre outros, e todos com o intuito de facilitar a compreensão dos conteúdos favorecendo, assim, o aprendizado dos alunos, tendo em vista, a construção do conhecimento aliando-se as TDICs.

A corrida digital ocasionada pela pandemia, que direciona o mundo para o online, não afetou apenas os alunos, mais os professores também, que precisaram adaptar os seus métodos e encontrar formas inovadoras de se reinventar utilizando as tecnologias digitais como ferramentas facilitadoras, ou seja, cooperar com a aprendizagem de conteúdos diversos, criar espaço de integração e comunicação, permitir novas formas de expressão criativa, realizar projetos e realizar reflexão crítica, logo as TDICs são ferramentas importantes para a resolução de problemas relacionados com a matemática. (BASTOS e BOSCARIOLI, 2020)

No entanto, ao mesmo tempo, tem havido discussões sobre o acesso desigual à tecnologia e boas conexões de internet, que são barreiras para a continuidade do ensino à distância, especialmente para os alunos mais desfavorecidos.

Em articulação com as dez competências gerais, a área de matemática na Base Nacional Comum Curricular (BNCC), apresenta oito competências específicas de matemática para o ensino fundamental, e a quinta competência é justamente sobre as tecnologias digitais, como afirma a BNCC (2018, p. 267) no qual, "Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados". Nessa competência busca-se destacar o uso de diferentes tecnologias para resolver, organizar e comunicar os avanços no uso dos argumentos matemáticos no decorrer do ensino fundamental e em continuidade no ensino médio, assim afirma a BNCC (2018):

> A BNCC da área de Matemática e suas Tecnologias propõe a consolidação, a ampliação e o aprofundamento das aprendizagens essenciais desenvolvidas no Ensino Fundamental. Para tanto, propõe colocar em jogo, de modo mais inter-relacionado, os

> conhecimentos já explorados na etapa anterior, a fim de possibilitar que os estudantes construam uma visão mais integrada da Matemática, ainda na perspectiva de sua aplicação à realidade. (BRASIL, 2018, p. 527)

Isto posto, é perceptível como as TDICs, pois se encontram com intensidade ao processo de ensino-aprendizagem que é essencial para a matemática. Segundo as Orientações Curriculares para o Ensino Médio (2000, p. 34), "[…], ela abre novas possibilidades educativas, como a de levar o aluno a perceber a importância do uso dos meios tecnológicos disponíveis na sociedade contemporânea". Nesse sentido, o uso das tecnologias digitais e computacionais no ensino da matemática, possibilita aos estudantes, desenvolver o pensamento computacional através da interpretação e aprimoramento de algoritmos (incluindo algoritmos que podem ser representados por fluxogramas), levando em conta as vivências cotidianas dos estudantes.

Em síntese, as tecnologias digitais no ensino-aprendizagem de matemática, possibilita uma abordagem mais significativa ao encontrar estudantes em sala de aula oriundos da cultura digital.

5 METODOLOGIA DA PESQUISA

Neste capítulo é apresentado o enquadramento metodológico da pesquisa, bem como as descrições dos processos de desenvolvimentos adotados.

5.1 Enquadramento da pesquisa

Quanto à finalidade, a pesquisa é Aplicada, para Prodanov e Freitas, (2013, p. 51), a pesquisa Aplicada, "Objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos. Envolve verdades e interesses locais". No panorama desta natureza de pesquisa, tem-se a proposta de estudo em abordar um tema com aplicações atuais, de um modo coerente, isto é, um tema mais compreensível para o aluno que esteja atrelado ao seu cotidiano.

De acordo com a forma de abordagem a pesquisa será mista, ou seja, quali-quantitativa. A abordagem qualitativa pode representar a complexidade de determinado problema, como a análise e relação de certas variáveis, compreender e classificar processos dinâmicos vividos por grupos sociais (RICHARDSON, 2015). A análise quantitativa caracteriza-se pelo emprego da quantificação, tanto nas modalidades de coleta de informações quanto no tratamento delas, por meio de técnicas estatísticas, desde as mais simples até as mais complexas. (RICHARDSON, 2015)

A abordagem mista é necessária para a análise dos dados deste estudo, porque trata-se de obter os objetivos na pesquisa, já que, é necessário compreender, analisar, discutir e vivenciar todo o processo que será desenvolvido como proposta em sala de aula.

Quanto aos objetivos optou-se pela pesquisa exploratória. A pesquisa exploratória possibilita aos pesquisadores adquirir maior familiaridade com o tema discutido, definindo os objetivos ou formulando as hipóteses de forma mais ampla. (DEL-MASSO, 2012)

Assim, a análise descritiva visa especificar os fatos mais pertinentes para avaliar os resultados esperados neste estudo.

Com relação, aos procedimentos metodológicos, apresentam características de Pesquisas Bibliográfica e estudo de Campo. O estudo de Campo a primeiro momento precisa realizar a Pesquisa Bibliográfica, segundo Prodanov e Freitas, (2013):

> Ela servirá, como primeiro passo, para sabermos em que estado se encontra atualmente o problema, que trabalhos já foram realizados a respeito e quais são as opiniões reinantes sobre o assunto. Como segundo passo, permitirá que estabeleçamos um modelo teórico inicial de referência, da mesma forma que auxiliará na

> determinação das variáveis e na elaboração do plano geral da pesquisa. (PRODANOV e FREITAS 2013. 59)

O estudo de campo tem a imprescindibilidade de verificação bibliográfica, como qualquer outro tipo de pesquisa. (PRODANOV e FREITAS, 2013)

As características dos procedimentos apresentados, são elementares para as atividades propostas neste estudo, visto que, foram expostos os aspectos históricos, conceitos atuais e essenciais para estudo da matemática, embasados em materiais já publicados, como: livros, dissertações, monografias, publicações em periódicos e artigos científicos, tendo o propósito de conduzir os pesquisadores ao contato direto com esses materiais. De acordo com Rodrigues, Batista e Teixeira (2019):

> É frequente, em textos acadêmicos, a discussão sobre as dificuldades de aprendizagem de conteúdos matemáticos. Parte dessas dificuldades está associada ao fato de que a maioria das metodologias de ensino da Matemática se reduz a um modelo de aulas expositivas, teóricas e abstratas no qual o professor se torna o centro e o aluno tem um papel de mero expectador.

Partindo deste conceito, propomos no presente trabalho que tem por objetivo utilizar a criptografia para relacionar teoria e prática, estabelecendo relações entre o desembaralhar de um código e as Funções Afins e suas Inversas, dando uma nova perspectiva da utilidade da matemática e familiarizar com os conceitos matemáticos envolvidos em seu funcionamento.

5.2 Proposta didática

O processo de criptografar e descriptografar uma mensagem pode ser relacionada a uma associação e desassociação de símbolos, e é justamente a palavra associação, de um ponto de vista intuitivo, que caracteriza as funções como sendo uma forma de associação. Do ponto de vista matemático, veremos a aplicação de uma função afim para criptografar uma mensagem e sua inversa para descriptografar a mensagem.

Para tanto, é necessário garantir que a função escolhida, seja invertível. E essa garantia se dá a partir da bijetividade, uma vez que somente as funções bijetoras possibilitam a volta ao contra domínio, permitindo assim que o processo seja desfeito. As funções que se enquadrem nesse critério, admite inversa.

A proposta didática consiste em: escolher uma mensagem e pré-criptogarfar, ou seja, convertê-la em números e criptografar através de uma função bijetora, e através de sua inversa

descriptografar esses números novamente para a mensagem original, como mostra os passos a seguir.

Passo 1: Escolher a mensagem

Uma vez que estamos trabalhando em um campo numérico, devemos associar biunivocamente, cada letra do alfabeto a um número. Dessa forma apresentamos a tabela 5 a seguir.

Tabela 5 – Pré-criptografia.

ESPAÇO	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
29	56	76	80	31	13	24	11	97	50	10	10	61	67
	N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
	87	1	90	62	21	3	**43**	15	69	41	89	84	19

Fonte: Dos autores, (2020).

Por exemplo, será pré-criptografada a mensagem MATEMATICA, as palavras serão substituídas pelos números correspondentes às letras que as compõem, como mostra a tabela 6.

Tabela 6 – Relação de cada letra da mensagem com seu respectivo número.

M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**C**	**A**
67	56	43	13	67	56	43	50	80	56

Fonte: Dos autores, (2020).

Passo 2: Escolher função

$$f(x) = 2x + 1$$

$$f(67) = 2\,.\,(67) + 1 = 135;$$

$$\cdots$$

$$\cdot$$

$$\cdot$$

$$\cdot$$

$$\cdots$$

e assim por diante, até criptografar o último número corresponde a última letra da mensagem escolhida.

Passo 3: Decifrar utilizando a Função inversa: $f^{-1}(x) = \frac{(x-1)}{2}$

$$f^{-1}(135) = \frac{(135-1)}{2} = 67;$$

$$\cdots$$

$$\cdot$$

$$\cdot$$

$$\cdot$$

$$\cdots$$

e assim por diante, até decifrar o último algoritmo, como mostra a tabela 7.

Tabela 7 – Mensagem decifrada.

135	**113**	**87**	**27**	**135.**	**113**	**87**	**101**	**161**	**113**
M	A	T	E	M	A	T	I	C	A

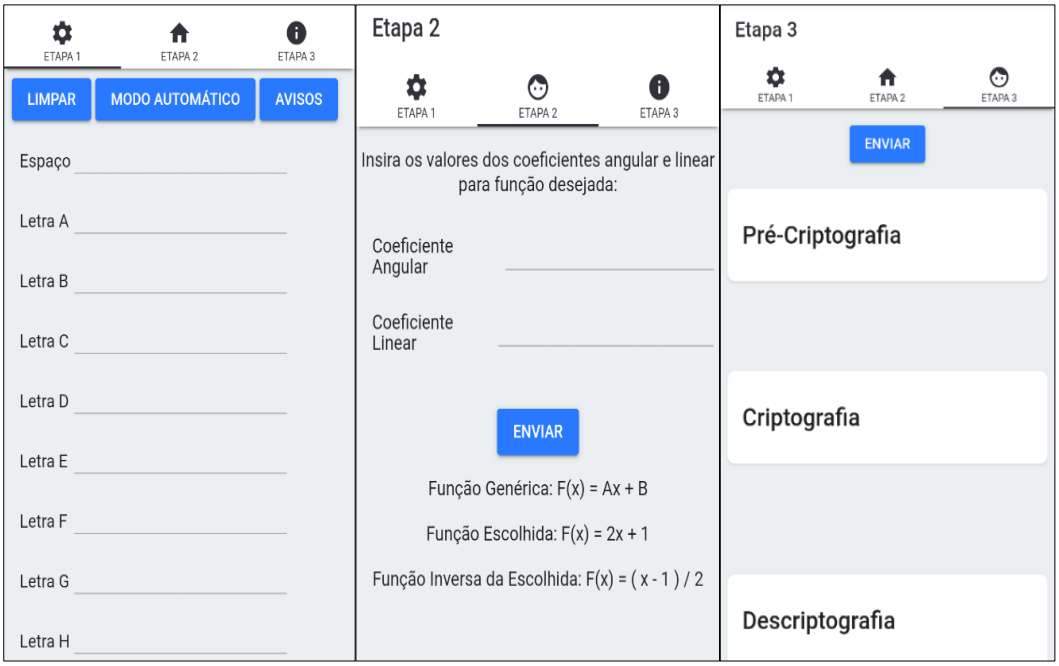
Fonte: Dos autores, (2020).

O interessante da criptografia é perceber que alguns dos números cifrados não existem na tabela e, caso o interceptador tenha acesso à tabela de associação, ele não conseguirá decifrar mensagens.

No entanto, percebe-se que está proposta torna-se um processo manual e mecânico no que se refere ao processo de identificar os números associados as letras, isto é, vai requerer muito tempo para a correção da tarefa do aluno em sala de aula.

Buscando uma metodologia alternativa para facilitar tal associação os autores desenvolveram o CriptoDática, um Software aplicativo que busca fazer essa associação de forma mais prática e didática, uma ferramenta com linguagem simples e moderna para dinamizar e automatizar o que antes seria um processo de correção braçal, racionalizando tempo para ser usado de uma melhor forma, podendo abranger toda a turma e ao mesmo tempo individualizar as tarefas pelos alunos em sala de aula. A figura 6 ilustra as interfaces das etapas do CriptoDática.

Figura 6 – Aplicativo Criptodática.



Fonte: Dos autores, (2020).

6 ESTRUTURA E FUNCIONAMENTO DO APLICATIVO CRIPTODÁTICA

Neste capítulo apresentaremos o software aplicativo desenvolvido para este estudo, intitulado CriptoDática, desenvolvido de forma a se tornar uma ferramenta para auxiliar o ensino de funções afins e suas inversas associadas ao tema criptografia.

O aplicativo CriptoDática ao todo é composto por três etapas dependentes e permite ao usuário a realização de pré-criptografar a mensagem, criptografar a mensagem e descriptografar a mensagem. O **CriptoDática** pode ser acessado através do endereço: http://ultratec.link/app/criptodatica/.

Apesar do aplicativo ter seu acesso disponível, acreditamos que ainda são necessários vários ajustes e melhorias, que busquem aumentar a gama de possibilidades quanto a sua utilização. Além disso, somente com o uso e colaboração dos usuários, será possível tornar o seu uso mais intuitivo e dinâmico.

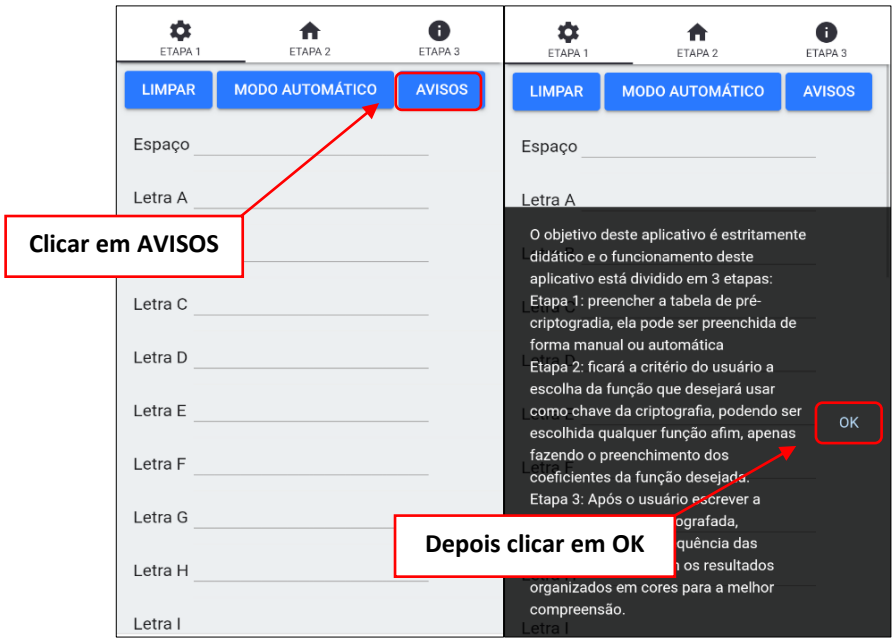
A figura 7, mostra a interface da primeira etapa do aplicativo, que é composta por uma tabela de vinte e sete linhas associadas a uma letra do alfabeto incluindo o espaço entre as palavras, representado na tabela como “espaço”, a primeira etapa também inclui as opções “limpar”, “modo automático”, “avisos” e “salvar”.

Figura 7 – Interface da primeira etapa do aplicativo.

Fonte: Dos autores, (2020).

Quanto as funções da primeira etapa, é importante que o usuário inicie a utilização após a leitura dos avisos, como mostra a figura 8.

Figura 8 – Destaque dos avisos na interface da primeira etapa do aplicativo.

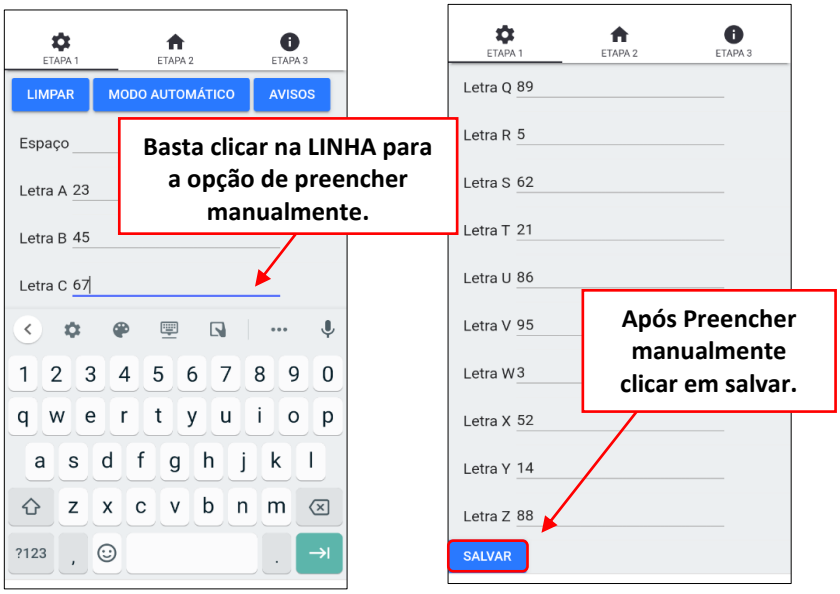


Fonte: Dos autores, (2020).

Os avisos são referentes as instruções de como realizar cada etapa, após a leitura do aviso o usuário deverá clicar em “OK” para iniciar a utilização do aplicativo.

Quanto ao preenchimento da tabela de pré-criptografia, há duas opções para fazer o preenchimento dela, pode-se preencher manualmente ou utilizar a opção “modo automático”, como mostra a figura 9 e 10.

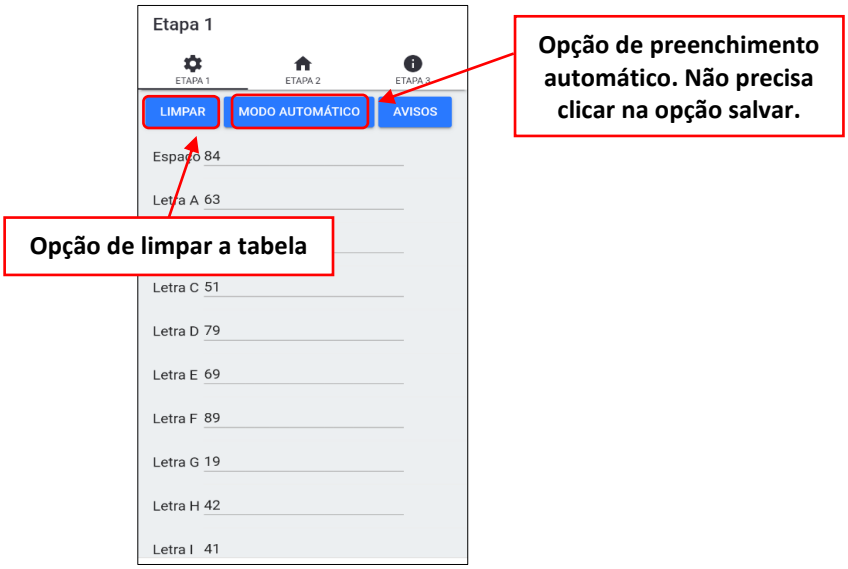
Figura 9 – Preenchimento manual da tabela de pré-criptografia da etapa 1.



Fonte: Dos autores, (2020).

A figura 10 mostra os procedimentos para o preenchimento automático, e para usá-lo basta usar a opção “modo automático”, nesta opção não é necessário clicar na opção “salvar” pois o salvamento é automático, além disso, o aplicativo dispõe da opção “limpar”, caso precise refazer a tabela.

Figura 10 – Opções limpar e modo automático da primeira etapa do aplicativo.



Fonte: Dos autores, (2020).

O Motivo de pré criptografar a mensagem, é simplesmente para associar números as letras do alfabeto, pois como o intuito é criptografar mensagens usando funções, e elas operam

somente com números, é preciso que os números aparecem de alguma forma, e a forma mais lógica é associar cada letra do alfabeto a um número, incluindo o espaço entre as palavras é preciso associá-lo a um número.

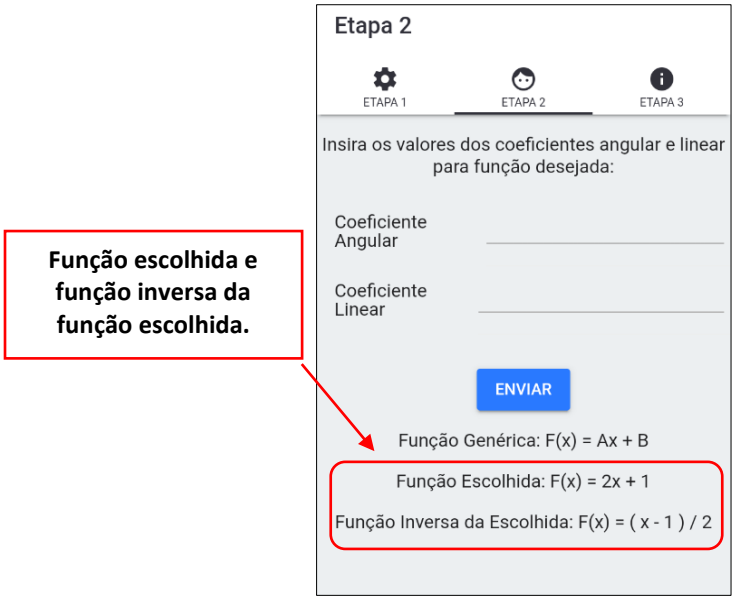
A figura 11 corresponde a “Etapa 2” do aplicativo, que é sobre a escolha da função afim para criptografar a mensagem, e para o coeficiente angular e linear existe uma alinha correspondente para inserir valores.

Figura 11 – Interface da Etapa 2 do aplicativo.

Fonte: Dos autores, (2020).

Nesta etapa o usuário deverá inserir os valores para os coeficientes angular e linear, e para inserir os valores basta clicar na linha correspondente ao coeficiente, após o preenchimento clique em “enviar”, após clicar nesta opção ele mostrará a função escolhida e automaticamente também mostrará a função inversa da função escolhida, como mostra a figura 12 a seguir.

Figura 12 – Inserção dos valores para os coeficientes da função.



Fonte: Dos autores, (2020).

O propósito de utilizar a criptografia como estudo da função Afim e Inversa é fazer com que os alunos consigam criptografar uma mensagem usando uma função e em seguida consigam descriptografar usando a função inversa da qual ele criptografou, e é justamente nessa etapa que o aluno escolherá a função para criptografar a tal mensagem, visto que, as letras já estão associadas aos números na etapa 1.

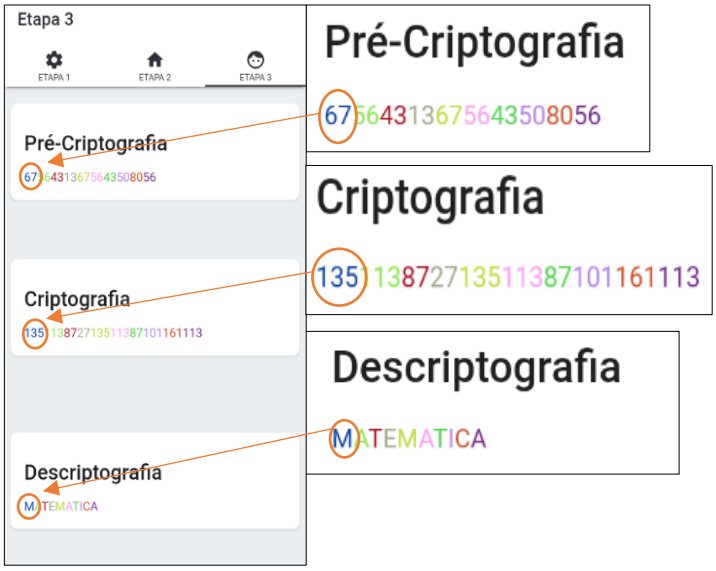
A "Etapa 3", trata-se da principal ideia do estudo, que é escolher a mensagem para aplicar as funções afins e inversas para criptografar e descriptografar. Para isso é necessário escolher uma mensagem como ilustra a figura 13.

Figura 13 – Escolher o texto para criptografar e descriptografar.

Fonte: Dos autores, (2020).

Após clicar em “enviar”, o aplicativo mostrará automaticamente a “pré-criptografia”, “criptografia” e “descriptografia”. E para facilitar o processo de correção do professor em sala de aula sobre quais números correspondem a letra da tabela de pré-criptografia, o aplicativo fará essa associação por cores, como mostra a figura 14 a seguir.

Figura 14 – Etapa três do aplicativo.



Fonte: Dos autores, (2020).

Na figura 14, destacam-se os números correspondentes as letras pelas cores, na palavra escolhida “MATEMATICA” à duas letras M (a primeira letra M é representada pela cor azul e a segunda letra M é representada pela cor amarela) a figura 11 destaca a primeira letra “M” que é representada pela cor azul, logo todos os números associados a primeira letra a M serão azuis.

Essa associação por cores agiliza o meio de correção do professor em sala de aula podendo abranger toda a turma, e ao mesmo tempo individualizar as tarefas pelos alunos em sala de aula com o ensino de Função Inversa.

6.1 Processo de desenvolvimento do aplicativo

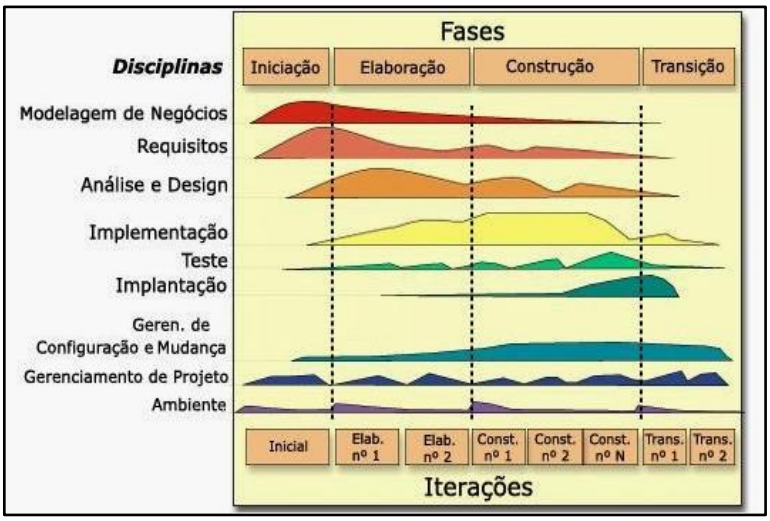
O processo de desenvolvimento do software aplicativo compreendeu as fases de planejamento didático-pedagógico, estudo e definição de tecnologias adequadas ao projeto, seleção de ferramentas para o processo de ciclo de desenvolvimento.

A engenharia de software responsável pela padronização dos processo de desenvolvimento de software recomenda o desenvolvimento através de um conjunto de fases. Cada uma das fases pode envolver métodos, ferramentas e procedimentos, cujas formas de

estruturação são citadas como modelo de engenharia de software (PRESSMAN, 2002). Ainda segundo Pressman (2002), independentemente do modelo de desenvolvimento de software, o processo contém três fases genéricas: definição, desenvolvimento e manutenção.

A aplicação seguiu os preceitos de engenharia de software dividido em etapas de desenvolvimento até a versão final do aplicativo, de acordo com o processo unificado de desenvolvimento de software, como mostra a figura 15.

Figura 15 – Gráfico de Baleias.



Fonte: Adaptado de KRUCHTEN, (2003).

O software aplicativo é baseado na plataforma *WEB* podendo ser aplicado nas diversas versões de sistemas operacionais e portado em diversos navegadores pela característica da responsividade o que torna altamente acessível e disponível a qualquer usuário.

A classificação do desenvolvimento é dividida em duas etapas compreendidas entre o *front-end* que representa as características visuais ou a interface com o usuário e a etapa de *back-end* que trata das funcionalidades efetivas que a software deve realizar em conjunto com a interface.

Em resumo para desenvolvimento dos componentes do *front-end* foi utilizado a plataforma *ONSEN Ui* 2.0 que trata dos elementos HTML, JS, CSS que realiza a interação humano-máquina, para o elemento de *back-end* foi utilizada a linguagem de programação orientada a objetos PHP em sua versão 7.3 para realizar o custeio das operações e integração dos componentes.

Para disponibilização na web a fim de dar acesso potencialmente a público foi utilizado a ferramenta *Apache* 2.4 que corresponde a um ferramenta de serviço de disponibilização de

sites para acesso comum, assim fechando o ciclo em conjunto com a etapa de testes para disponibilização.

O Webapp (mas conhecido por aplicativo(s) web) se derivam do *Progressive Web Apps* (PWAs) são tecnologias recentes, que significativamente contribuem com a crescente dos aplicativos mobile e consequentemente o conteúdo móvel, oferecendo ao usuário uma experiência multiplataforma, através de uma infinidade de recursos da web que foram previamente alocados para aplicativos nativos.

O termo PWA, segundo indicam Biorn-Hansen, Majchrzak e Gronli (2017), que elencam características que descrevem essa nova forma de apresentar o conteúdo online: progressiva, responsiva, independente de conectividade, semelhante a um aplicativo, nova, segura e detectável são algumas características deste novo modelo e forma de aplicativos não nativos.

7 RESULTADOS E DISCUSSÕES

Segue o enquadramento dos resultados e discussões da pesquisa, para a avalição da proposta didática e do CriptoDática apresentados neste estudo, bem como os procedimentos de coleta e análise de dados.

Para a produção dos dados desta pesquisa primeiro houve a apresentação do CriptoDádita por meio de um vídeo tutorial disponível em: https://drive.google.com/file/d/1gpq6ayigcglcq0zbttvtfw0rdxucnkdv/view?usp=sharing, juntamente com a proposta didática. Posteriormente, os pesquisados foram convidados a responder um questionário através de uma plataforma digital online, *Google forms*. Esse questionário foi respondido por 40 (quarenta) professores de matemática que atuam na cidade de Macapá no estado do Amapá. O convite para responder o questionário foi enviado por meio de *emails* em outubro de 2020.

7.1 Análise dos dados

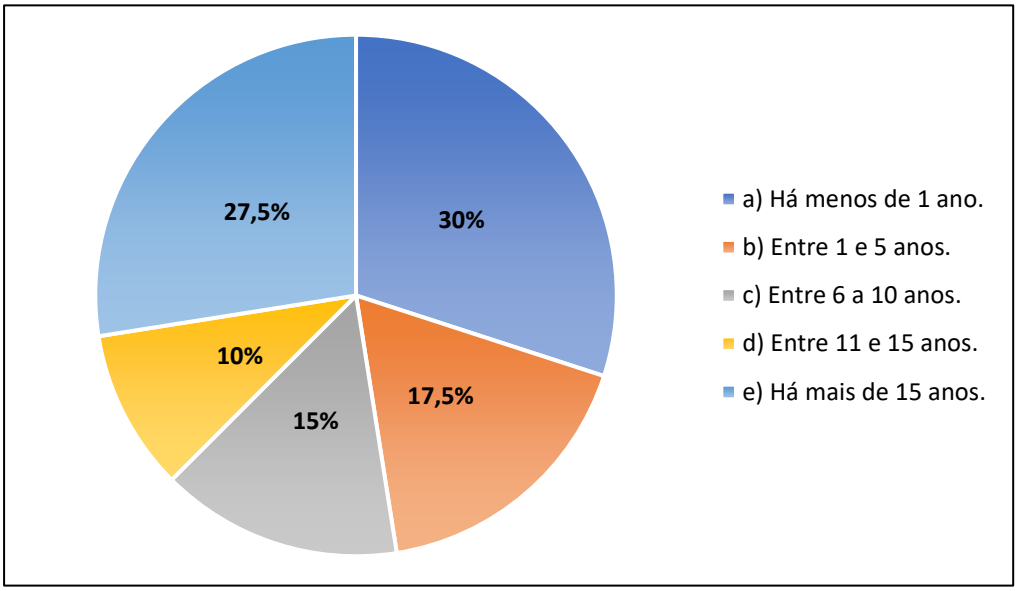
O questionário foi organizado em 13 (treze) questões por dois eixos, o primeiro eixo é sobre o perfil dos professores, relativo as variáveis laborais, como titulação mais elevada e tempo de docência, como também a experiência na atuação em sala de aula. O segundo eixo é sobre a avaliação feita do aplicativo CriptoDática, para uma a análise que converge para um conhecimento necessário em relação a compreensão dessa ferramenta proposta.

Os resultados foram divididos em perguntas compreendidas como abertas e fechadas e em escala de níveis classificatórios de 0 a 5, na qual a escala 0 indica discordar plenamente e a escala 5 significa concordar totalmente. Com o intuito de analisar os resultados a partir da experiência com a disciplina Matemática com temas geradores e de tecnologias digitais de informação e comunicação e o que eles poderiam dizer aos pesquisadores concluintes do curso de Licenciatura em Matemática. Salienta-se que nessa escrita foram abordadas as questões principais coletadas no questionário.

7.1.1 Perfil dos professores

Em relação as variáveis laborais dos professores sobre o tempo que atuam na docência, são possíveis verificar no gráfico 1, na qual 30% atua há menos de um ano; 17,5% atuam entre 1 a 5 anos; 15% entre 6 a 10 anos; 10% entre 11 a 15 anos e 27,5% a mais de 15 anos.

Gráfico 1 – Há quanto tempo atua como professor(a) de matemática?



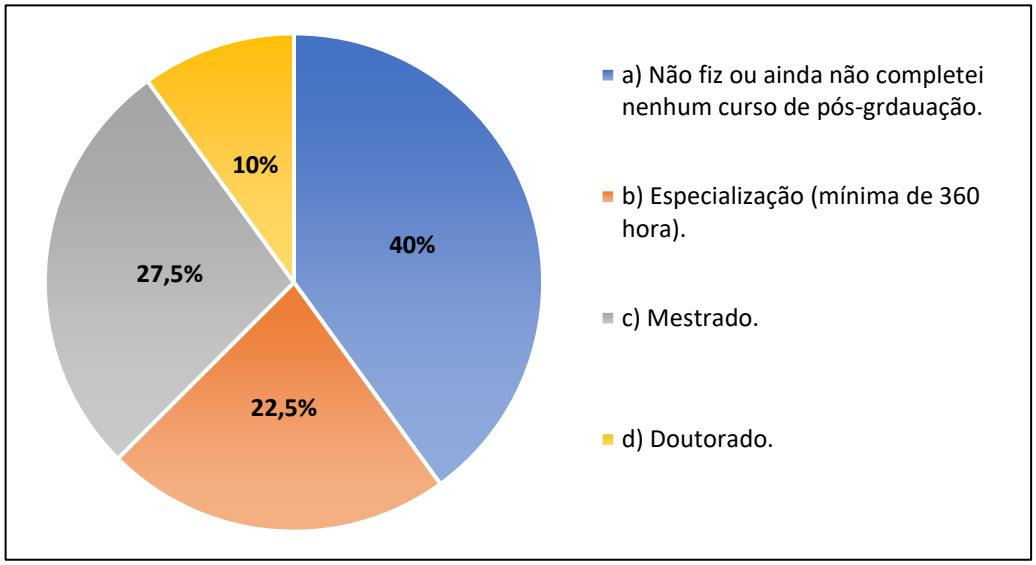
Fonte: Dos autores, (2020).

Sobre os professores que lecionam há menos tempo, que é justamente o professor de matemática em início de carreira, para Santana (2016, p.16), “os primeiros anos de profissão são decisivos na estruturação da prática profissional do professor e podem levar ao estabelecimento de rotinas e incorporação de conceitos (referentes à atividade docente) que tendem a influenciar fortemente toda a sua carreira”. Quanto aos que atuam há mais tempo, esses profissionais acumulam experiencias fundamentais que é transformada numa maneira pessoal de ensinar e como seu trabalho pedagógico vem sendo realizado no contexto atual da educação num âmbito de recursos digitais, sobretudo como se dá a coligação ensino-aprendizagem diante das novas exigências para a área, buscando refletir sobre uma educação significativa.

Na ocasião em que é iniciado a graduação em licenciatura em matemática, o processo de estruturação como professor acontece ao longo de um currículo que inclui disciplinas relacionadas à formação matemática e didático-pedagógica. Ou seja, percebe-se que o domínio de conceitos matemáticos não basta para o exercício da docência, isso significa que se deve começar atribuir significados às experiências vividas adotando um profissionalismo dentro dos contextos em que se participa.

Sobre o gráfico 2, corresponde ao curso de mais alta titulação que os professores participantes concluíram, e entre eles 40% não fez ou ainda não completou nenhum curso de pós-graduação, 27,5% possuem título de mestrado, 22,5% especialização e 10% possuem título de doutorado.

Gráfico 2 – Entre os cursos de pós-graduação listadas abaixo, assinale a opção que corresponde ao curso de mais alta titulação que você completou.



Fonte: Dos autores, (2020).

A formação continuada é importante para o desenvolvimento profissional que compreende a necessidade de transição e que busca aperfeiçoar-se naquilo que faz, desta forma, mantendo-se em sintonia com as tendências da educação. A mesma percepção é expressa por Albuquerque e Gontijo (2013, p. 76), “Por meio do processo de formação inicial e continuada, o professor constrói e reconstrói conhecimentos que, articulados com sua prática cotidiana, gerará saberes que o nortearão em sua tarefa primordial, o ensinar”.

Entende-se que a educação e o encargo docente, passaram a ser vistos como essenciais na formação do novo profissional na atualidade digital globalizada, além disso, segundo Silva (2019):

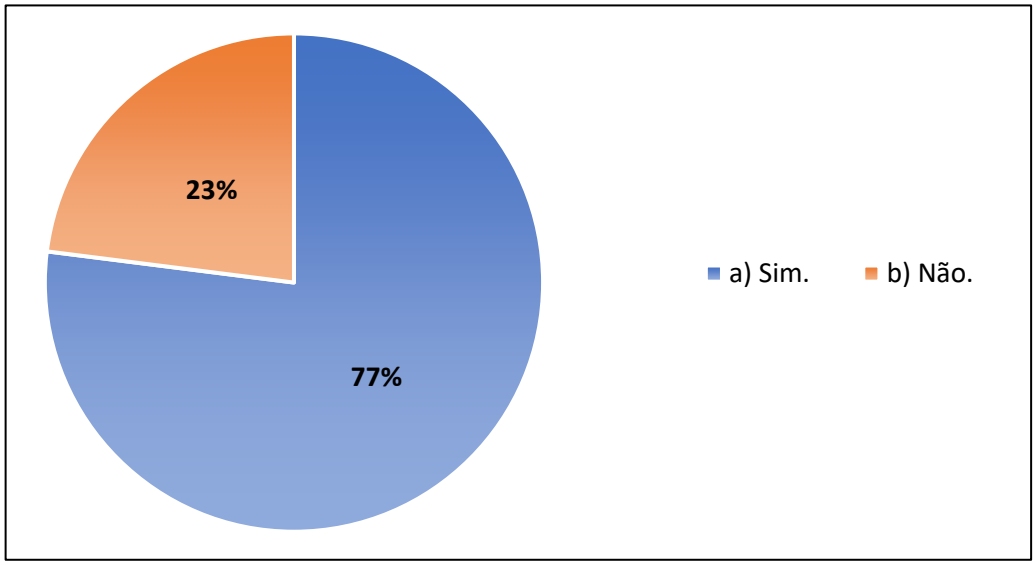
> […], a sociedade tem delegado à escola a função de formar sujeitos capazes de promover seu próprio aprendizado. Sendo assim, o professor julga-se no dever de se manter atualizado, objetivando ensinar de um modo diferente, já que o processo de ensino tradicional visto nas escolas se tornou desestimulante e arcaico para os estudantes. (SILVA, 2019, p. 22)

Em função disso, é necessário que o professor de matemática possa garantir essa expansão de inovação e reconstrução do modelo tradicional de ensino. objetivando o aprimoramento do ensino de disciplinas fundamentais com intuito de proporcionar à boa formação dos estudantes inseridos nesta realidade.

O gráfico 3, expõe os dados coletados sobre as Tecnologias Digitais de Informação e Comunicação (TDICs), na qual, foram perguntados aos professores participantes se, durante sua formação acadêmica experienciaram em componentes curriculares esse eixo tecnológico,

resultando em mais de 77%, assinalando que“Sim” e 23% assinalaram que “não” sobre o contato com a TDICs.

Gráfico 3 – Em sua formação acadêmica você teve contato com as componentes curriculares nas quais tenham estudado as TDIC's?



Fonte: Dos autores, (2020).

Esse é o reflexo das políticas públicas que surgem tendo como um dos objetivos de formar o docente para integrar as tecnologias digitais de informação e comunicação (TDICs) no ensino básico, e este objetivo é evidenciado no trabalho de pesquisa de Nishio e Hora (2018, p. 78), e afirmam que, “No processo de formação de professores de Matemática é necessário ter como um dos objetivos, o domínio de algumas ferramentas digitais”, ou seja, referem-se ao domínio da prática que envolve o uso dos recursos tecnológicos que mediam a construção de conhecimentos relacionados a matemática.

O professor em formação com interação por meio das TDICs integradas à educação, preveem cenários de ensino e aprendizagem transformadores, em que, mostram uma progressiva reinvenção e inovação de suas metodologias, ou seja, uma possibilidade de ampliar as perspectivas da produção de situações de aprendizagem que favoreçam o processo de construção do conhecimento matemático, em diferentes eixos da matemática, da educação básica ao ensino superior.

Por outro lado, ainda nos deparamos com uma escola do século XIX e práticas pedagógicas do século XX, no qual, se vive em uma atualidade que é caracterizada pela geração tecnológica denominada por alguns autores como nativos digitais. Sobre os nativos digitais, trata-se da geração imersa no contexto digital, tendo uma intensa relação com os dispositivos e

aplicativos que surgem e se desenvolvem em uma velocidade frenética, cujo resultado dessa interação reflete na forma como elas pensam e processam informações alterando de forma singular toda uma geração. (CAVALCANTE 2020)

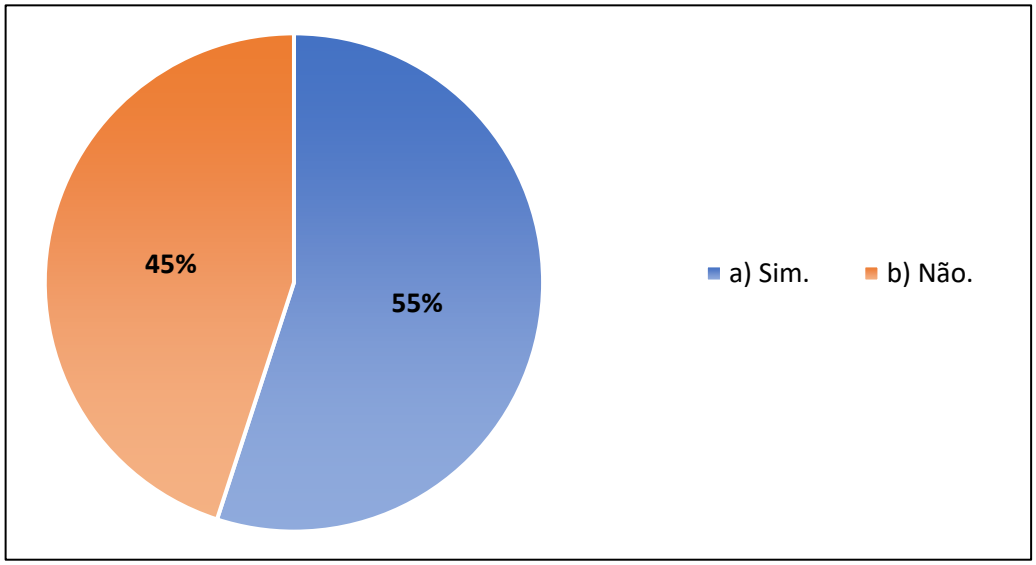
Contrário ao novo cenário social, existe os imigrantes digitais, que são aqueles não nascidos dentro deste universo tecnológico. Isto é, os que foram inseridos nele, por conveniência, imposto ou necessidade, bem como, a realidade do professor, de como se adaptar no contexto digital social, muitas vezes trazendo consigo hábitos e vícios tradicionais enraizados a sua essência. De acordo com Samá, Moura e Santos (2020):

> A maioria dos professores que atua nas escolas, em geral, imigrantes digitais, encontra dificuldade em lidar com as rápidas mudanças tecnológicas. Ademais, os cursos de formação de professores pouco têm incluído, em sua proposta curricular, disciplinas que promovam a reflexão acerca dos modos interativos e instigantes de ensinar e aprender. (SAMÁ, MOURA e SANTOS, 2020, p. 20)

À vista disso é interessante que os cursos de formação de professores considerem o potencial desses recursos tecnológicos do novo cenário social em suas componentes curriculares, tendo em vista o não distanciamento do ambiente escolar da realidade do estudante.

O gráfico 4, trata-se de conteúdos matemáticos trabalhados a partir de temas geradores e se os professores trabalham ou já trabalharam nessa perspectiva, bem como, exemplificar temas e conteúdo, em que 55% marcaram que “Sim” e 45% marcaram “Não” nessa questão apresentada.

Gráfico 4 – Você trabalha ou trabalhou conteúdos matemáticos a partir de um tema gerador? Se sim, exemplifique.



Fonte: Dos autores, (2020).

Observa-se a partir da análise dos dados apresentadas no gráfico 4, que os professores utilizam temas geradores adotados, sugeridos com base no estudo e análise da realidade da comunidade escolar que estão inseridos.

O uso de tema gerador ou a integração temática interdisciplinar desenvolvida pelos educadores, através de projetos potencializados e de um jeito que lhe seja mais significativo são algumas das formas que os educadores encontraram para praticar um modelo de educação mais próximo possível da realidade do aluno.

Mendes (2010), da mesma forma relata sobre trazer a realidade cotidiana para dentro da sala de aula:

> Há algum tempo, a procura de alternativas didáticas que pudessem superar as dificuldades encontradas no processo de ensino e de aprendizagem de ciências e matemática fizeram com que alguns estudiosos da área de educação buscassem uma relação dinâmica na qual a realidade se constituísse no elemento gerador do conhecimento ensinado e aprendido em sala de aula. (MENDES, 2010, p. 574)

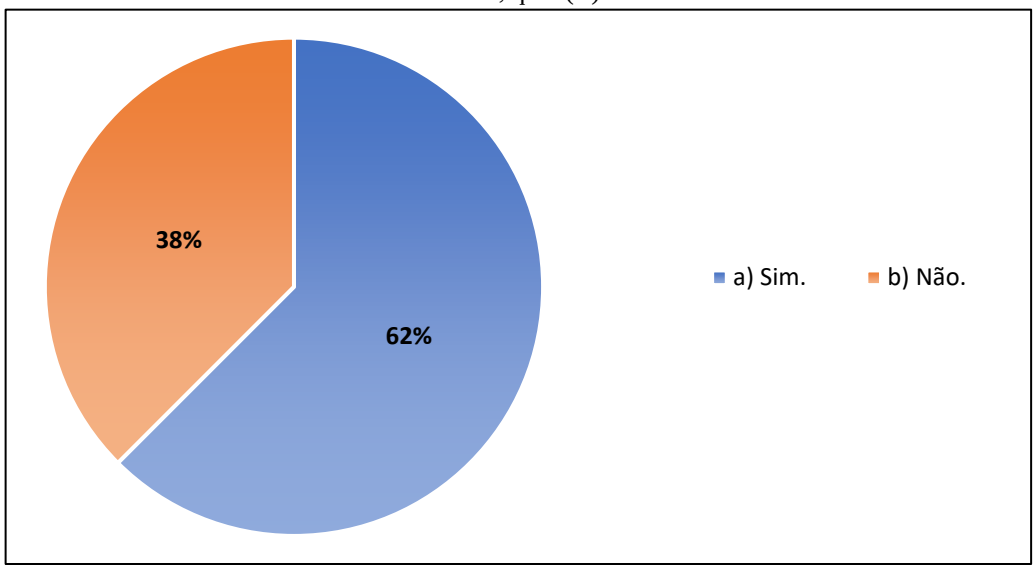
O conhecimento cotidiano não aparece desveladamente. É constituído, igualmente, de saberes matemáticos que aparecem das situações do meio em que os indivíduos estão envolvidos, isto é, nas relações com as diferentes vivências.

Isto posto, entende-se que para mudar o estigma de que a matemática é um assunto difícil de ser compreendido, deve-se por meio da intervenção de elaboração de temas motivadores e/ou geradores rompendo essas associações negativas da matemática.

Nesta questão que mostra o gráfico 5, foram perguntados aos professores, se: conhecem ou utilizam softwares e/ou aplicativos voltados para o ensino de funções. E para a alternativa “Sim” 62% assinalaram conhecer ou utilizar softwares e/ou aplicativos voltados para o ensino de funções, e 38% assinalaram a alternativa “Não”.

E para os que assinalaram que “Sim” foi solicitado que informassem quais softwares e/ou aplicativos que aplicam em sala de aula para o ensino de funções.

Gráfico 5 – Você conhece ou utiliza softwares e/ou aplicativos voltados para o ensino de funções? Se sim, qual (is)?



Fonte: Dos autores, (2020).

Os softwares e/ou aplicativos demandam conhecimentos diversos os quais são necessários para que o professor de matemática possa ensinar. Goodwin (2017) refere-se a esses conhecimentos como:

> [...] possuir conhecimento teórico de sua disciplina e estar disposto a utilizar novas ferramentas de ensino. Estas devem favorecer o desenvolvimento de habilidades e procedimentos pelo professor, visando orientar seus alunos a conviver num ambiente cada vez mais tecnológico. (GOODWIN, 2017, p. 48)

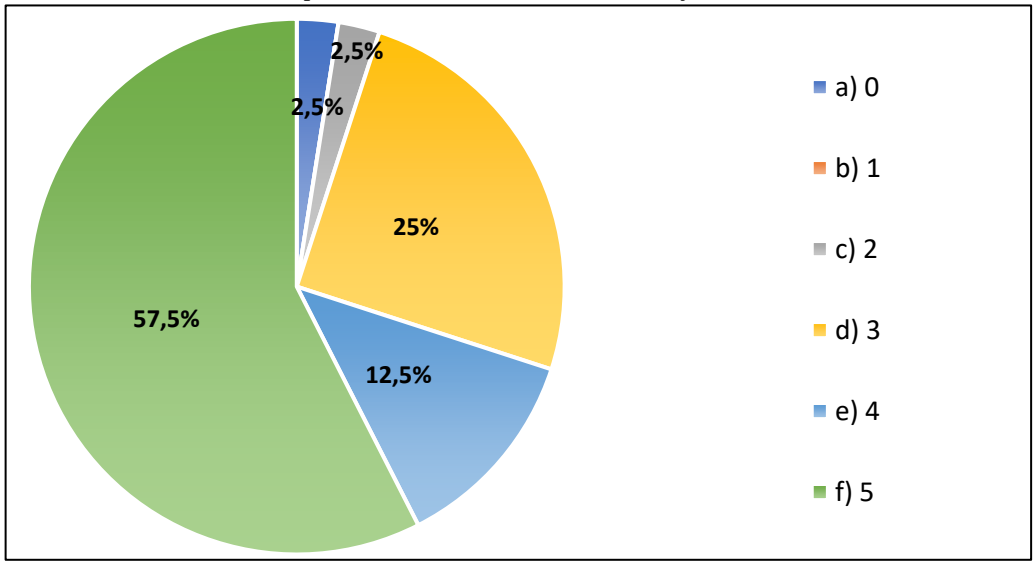
Em vista disso, o professor tem o papel de guiar seus alunos ao encontro da construção do conhecimento. Mas, integrar esses conhecimentos com softwares e/ou aplicativos em sala de aula, o professor para exercer essa função é preciso que ele seja detentor de conhecimentos não apenas os tecnológicos e/ou matemáticos, mas, da mesma forma os pedagógicos, num entendimento integrador gerando um novo tipo de conhecimento.

Entre os softwares e/ou aplicativos para o ensino de funções que os professores indicaram no questionário, o GeoGebra foi o mais indicado por eles. O GeoGebra trata-se de um recurso de geometria dinâmica em que se pode verificar e visualizar mais rapidamente o comportamento de uma função no plano cartesiano, é também um software livre para todos os níveis de ensino permitindo elaborar construções geométricas com a aplicação de ponto, reta, plano, polígono, sólidos e outros.

Além do GeoGebra, foram indicados mais outros softwares e/ou aplicativos para utilizados para o ensino de funções, tais como: *Winplot;* Função de gráfico *plotter*; *CALC;* Plataforma MIT APP Inventor; Excell e Calculadoras de funções on line.

Considerando o tema criptografia para ser abordado no ensino de funções, o gráfico 6, mostra o nível de uma escala de 0 a 5, na qual 0 indica discordar plenamente e 5 concordar totalmente. Sobre considerar esta abordagem 55% assinalaram a escala 5, seguido de 12,5% para escala 4, escala 3 com 25%, escala 2 com 2,5%, escala 0 com 2,5% discordando plenamente e ninguém assinalou a escala 1.

Gráfico 6 – Em uma escala de 0 a 5, em que nível você consideraria o tema criptografia para ser abordado no ensino de funções?



Fonte: Dos autores, (2020).

Nota-se que o tema criptografia para o ensino de funções é considerado pelos professores porque este tema apresenta-se com muita aplicabilidade coerente, interessante e atual da matemática, inclusive em algumas coleções de livros didáticos apresentam o tema criptografia com um conceito matemático. Litoldo e Lazari (2014, p. 154), falam de livros didáticos que abordam o tema criptografia para fixar e complementar o aprendizado do assunto de funções, “A Criptografia vem tendo destaque nas notícias da atualidade, aproximando ainda mais os alunos, e a população em geral deste tema, o que pode estimular a difusão entre os autores dos Livros Didáticos da sua conexão com alguns conceitos matemáticos.”

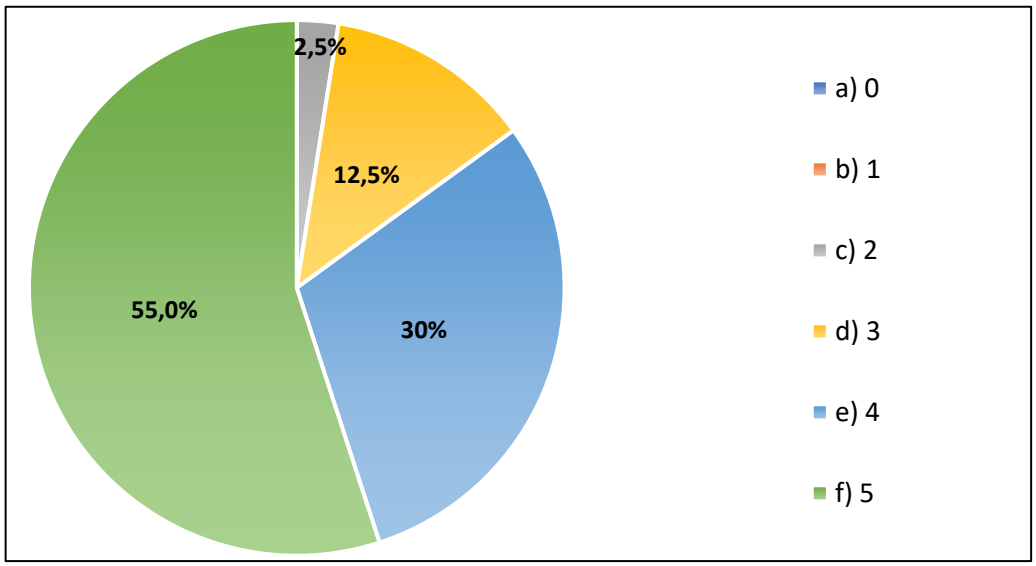
No entanto, os Parâmetros Curricular Nacional (PCN) e a Base Nacional Comum Curricular (BNCC), ou seja, os documentos oficiais apresentados pelo Ministério da Educação, não falam claramente a respeito do tema criptografia, mas salientam a respeito do desenvolvimento de diversos modelos de raciocínios.

7.1.2 Avaliação feita do aplicativo CriptoDática

Agora, a respeito da proposta do web aplicativo intitulado CriptoDádita, observamos, de modo mais detalhado, a análise que converge para um conhecimento necessário em relação a compreensão dessa ferramenta após a avaliação feita pelos professores participantes do questionário.

De modo geral, a escala de 0 a 5, não apresentou nenhuma nota 0 e 1, o que caracterizaria discordar plenamente de alguma afirmação. Isso trouxe resultados expressivos quanto a satisfação do usuário e a relevância do conteúdo trabalhado no software CriptoDádita conforme mostra o Gráfico 7, bem como, os níveis de aceitação que iniciam na escala 2 com 2,5%, escala 3 com 12,5%, escala 4 com 30% e a escala 5 de nível mais alta indicando 55% em que os participantes consideraram relevante a utilização da ferramenta proposta neste estudo.

Gráfico 7 – Em uma escala de 0 a 5, em que nível a utilização do web aplicativo como ferramenta na sua visão poderia contribuir para a realização de atividades mais dinâmicas em sala de aula?



Fonte: Dos autores, (2020).

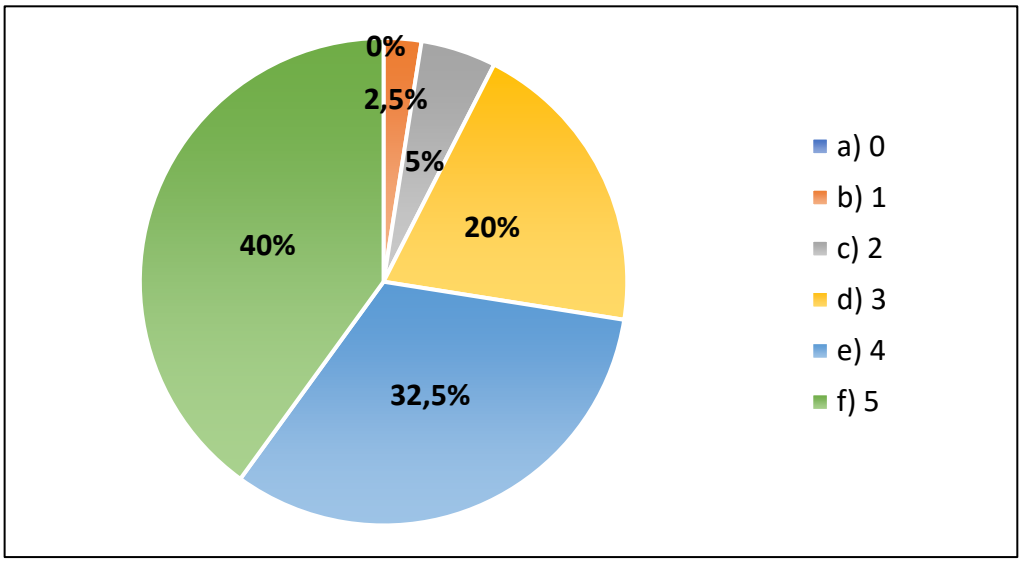
Fundamentado nesses resultados ressalta-se que, empregar novos recursos didáticos no contexto educacional é essencial, principalmente na nova rotina de estudos ocasionada pelo efeito da pandemia do novo Corona vírus (COVID-19), esse momento em que o uso das tecnologias se faz tão presente no cotidiano desse público, no qual, o professor também, devendo adaptar sua prática de ensino ao uso de recursos tecnológicos, precisou mobilizar novos conhecimentos, ferramentas didáticas manuseando recursos digitais para ministrar os conteúdos matemáticos. Segundo da Silva e Filho (2020):

> No entanto, nota-se que pouco ou quase nenhum esforço é realizado de fato para a adoção de softwares educacionais nos vários níveis do ensino nacional. Outro fato marcante é a necessidade de metodologias que extrapolem os métodos tradicionais de ensino, essa necessidade advém de um cenário de pandemia que trouxe consigo vários desafios para o ensino. O principal deles é o ensino à distância e a necessidade de prender a atenção dos estudantes, fazendo com que os mesmos absorvam os conteúdos lecionados. (DA SILVA e FILHO, 2020)

Considerando esse fato, o CriptoDádita atendeu com sucesso às condições propostas podendo contribuir para a realização das aulas em atividades mais dinâmicas, juntamente justificando para o aluno onde e como a matemática é empregada na temática criptografia em nosso cotidiano com objetivos de exercitar, aprofundar e revisar o conteúdo de funções Afins e Inversas.

Conforme mostra o gráfico 8, os resultados obtidos após a avaliação feita pelos professores participantes do questionário, que considerariam usar o CriptoDádita em questões propostas relacionadas a criptografia e inversão de funções como ferramenta em suas aulas, obteve-se como resultado 2,5% para a escala 1, escala 2 com 5%, escala 3 com 20%, escala 4 com 32,5% e a escala 5 com 40%, e ninguém assinalou a escala 0, o que significaria discordar plenamente quanto ao que foi perguntado.

Gráfico 8 – Em uma escala de 0 a 5, em que nível você utilizaria este aplicativo como ferramenta em suas aulas?



Fonte: Dos autores, (2020).

O método de avaliação para o CriptoDádita utilizado neste trabalhado foi elaborado buscando medir o grau de atendimento do aplicativo ao objetivo proposto pelo projeto que é utilizar a criptografia para relacionar teoria e prática, estabelecendo relações entre o desembaralhar de um código e as Funções Inversas, na perspectiva da utilidade da matemática

envolvidos em seu funcionamento. Carvalho (2020 p. 14), afirma que, “Entre os conteúdos matemáticos que são vistos pelos alunos do ensino médio um dos mais difíceis é o que aborda sobre funções”. E, é nesta perspectiva que o tema criptografia acaba aguçando a curiosidade e levando a uma metodologia que possibilita ao educando a construção de novos conhecimentos.

Os professores participantes desta pesquisa consideraram que o aplicativo veio somar em termos de contribuição para o desempenho na abordagem do conteúdo de funções. A aceitação presente na investigação sobre a ferramenta proposta neste estudo é muito importante para avaliar e analisar a situação didática na qual, busca-se dar continuidade no método de codificar e decodificar mensagens que se baseia num método de fazer e desfazer algo, o que equivale como princípio da função inversa.

Além disso, é possível e interessante que o estudante seja instigado com atividades gradualmente mais complexas com a utilização do CriptoDática, tendo em vista seu desenvolvimento intelectual, por exemplo: Identificar a chave de decodificação da mensagem; construir com o auxílio de um aplicativo o gráfico das funções de codificação e decodificação da mensagem; comparar o conjunto domínio e imagem das duas funções, entre outros.

Desta forma, a abordagem do ato de criptografar com o auxílio da ferramenta CriptoDática expostas neste estudo pode conceber um bom recurso pedagógico para que os professores utilizarem, principalmente, no desenvolvimento de atividades didáticas referentes ao conceito de função Afim e Inversa.

8 CONSIDERAÇÕES FINAIS

A criptografia no passado, foi amplamente utilizada como tática de guerras e por governos para facilitar as comunicações secretas. Hoje sua aplicação é comum para o sigilo e segurança em vários tipos de sistemas digitais civis.

Fundamentada com o seu rico passado histórico, a Criptografia atualmente é uma essencial ferramenta do estudo de sistemas de construção de algoritmos matemáticos. Ao ter fundamentos matemáticos, a criptografia baseia-se em princípios e técnicas ao codificar e decodificar mensagens que compreende um processo de fazer e desfazer algo, o que é similar ao princípio da função inversa.

No decorrer desse trabalho delineou-se resultados de um estudo envolvendo a proposta de associar o tema Criptografia ao conteúdo de Funções, mais especificamente função Afim e sua Inversa, na qual, é apresentado o CriptoDática, um aplicativo que busca trazer essa associação de forma mais prática. Para tal, procurou-se responder às seguintes questões da pesquisa: Como dinamizar, estimular e dar variabilidade na aplicação de questões propostas relacionadas a Criptografia e Inversão de Funções através do uso de um software?

Para responder tais questões, foi aplicado um questionário de avaliação, cujo objetivo foi esquematizar as opiniões dos professores pesquisados, e desta forma, buscou-se com os dados obtidos, compreender através de sua experiencia e seu fazer pedagógico, uma verificação que converge para as considerações da ferramenta CriptoDática, em que suas aplicações possam contribuir na resolução de problemas envolvendo Função Afim e suas Inversas.

É importante destacar que, utilizando os conhecimentos pré-existentes dos alunos, a contextualização proporcionada pelo tema Criptografia apresentada neste estudo seja capaz de despertar a motivação e interesse destes, ao perceberem que o processo, aparentemente mecanizado, do cálculo da inversa de uma função afim tem sentido e significação.

Como um resultado, a proposta da ferramenta CriptoDática apresentou ser aceitável, visto que, os professores pesquisados consideraram útil, uma vez que a utilização do CripitoDática, bem como, com as devidas adaptações e correções futuras, possa potencializar a associação do estudo do tema Criptografia com o assunto de Funções Afins e suas Inversas.

Para estudos futuros, como extensões deste trabalho, sugere-se a utilização do CriptoDática como ferramenta de pesquisas de campo em sala de aula para que alunos e professores avaliem a utilização desta ferramenta nas atividades de ensino-aprendizagem, bem como, podem ser elaboradas novas versões, tais como, a função exponencial e logarítmica; além

de enfatizar os conceitos de domínio, conjunto imagem das funções e outros objetos de aprendizagem com novos temas voltados a criptografia para atingir novos públicos.

Por fim, espera-se com este estudo, possa incentivar mais pesquisas sobre uso da contextualização permitindo reflexões sobre a Criptografia e o estudo das Funções, para aguçar o ensino da Matemática, de forma que haja o entendimento da matemática presente no atual cenário social.

REFERÊNCIAS

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, 2018.

BRASIL. **Orientações curriculares para o ensino médio: Ciências da natureza, matemática e suas tecnologias.** VOL 2. Secretaria de Educação Básica. – Brasília: Ministério da Educação, Secretaria de Educação Básica, 2006. 135 p.

BRASIL. Secretaria de Educação Fundamental**. Parâmetros curriculares nacionais: matemática**. Secretaria de Educação Fundamental. – Brasília: MEC/SEF, 1997, 142 p.

ALBUQUERQUE, L.; GONTIJO, C. A complexidade da formação do professor de matemática e suas implicações para a prática docente. **Revista Espaço Pedagógico**, v. 20, n. 1, Passo Fundo, p. 76-87, jan./jun. 2013. Disponível em: https://doi.org/10.5335/rep.2013.3508 . Acesso em 20 dezembro de 2019.

ÁVILA, Geraldo. **Introdução ao Cálculo**. Rio de Janeiro: LCT, 2012, 300p.

BASTOS, T. B. M. C. e BOSCARIOLI, *C.*2020. **Os Professores do Ensino Básico e as Tecnologias Digitais: Uma reflexão emergente e necessária em tempos de pandemia**. ISSN: 2175-9235. Disponível em: http://horizontes.sbc.org.br/index.php/2020/04/22/professores-do-ensino-basico-e-as-tecnologias-digitais/ . Acesso em: 29 de abril 2020.

BERLINGHOFF, W. P.; GOUVÊA, F. Q. A Matemática Através dos Tempos: um guia fácil e prático para professores e entusiastas. 2 ed. São Paulo: Blucher, 2010.

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

BIORN-HANSEN, A.; MAJCHRZAK, T. A.; GRONLI, T. (2017). Progressive Web Apps: The Possible Web-native Unifier for Mobile Development. In: WEBIST. p. 344-351.

BUENO, R. W. S.; BALLEJO, C. C.; VIALI, L. Entrando na zona de risco: utilizando as TDIC para ensino e aprendizagem de conceitos de estatística descritiva. **Revista Sergipana de Matemática e Educação Matemática** - ReviSeM, Itabaiana – Sergipe**,** vol. 5 n. 1, p. 71-88, 26 de abril de 2020. Disponível em : https://seer.ufs.br/index.php/ReviSe/article/view/12401 . Acesso em: 29 de novembro de 2020.

CANECO, Mário Augusto de Araujo. Criptografia e Matemática: Onde e Como Usarmos essa Interdisciplinaridade? **O Adjunto,** Cruz Alta -RS, v. 7, n. 1, p 149-155, nov. 2019. Disponível em: http://ebrevistas.eb.mil.br/index.php/adj/article/view/3229/2598 . Acesso em: 01 setembro de 2020.

COUTINHO, Severino. **Criptografia**. Rio de Janeiro: IMPA, 2014. 217 p.
DANTAS, Andréa de Araújo. **A Criptografia no Ensino Fundamental e Médio**. Monografia (Curso de Especialização em Ensino de Matemática para Ensino Médio) – Universidade Federal do Rio Grande do Norte, Caicó, 2016.

DANTE, Luiz Roberto. **Matemática: Contexto e aplicações (ensino médio).** 3ª Ed. São Paulo: Ática, 2016. 287 p.

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

FIGUEIREDO, Luiz Manoel. **Introdução à Criptografia**. v. 2. Rio de Janeiro: UFF / CEP – EB, 2010. 172p.; 21 x 29,7 cm.

GIL, A. C. **Como elaborar projeto de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GOODWIN, Fernanda Coelho. A utilização do software geogebra no tablet para o estudo das funções. **Revista Formação Docente**, Belo Horizonte, v. 9, n. 3, p. 46-56, 2017. Disponível em: https://doi.org/10.15601/1098 . Acesso em: 01 de novembro de 2020.

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

JANOS, Michel. **Matemática e natureza**. São Paulo: Livraria de Física, 2009. 419 p.

JESUS, André Luís Neris de. **Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes**. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Vale do São Francisco, Campus Juazeiro, Juazeiro-BA, 2013, xii, 70 f. : il ; 29cm.

KRUCHTEN, P. **Introdução ao RUP: Rational Unified Process.** Rio de Janeiro: Ciência Moderna, 2003.

LIMA, Elon Lages. **Matemática e Ensino**. 3 ed. Rio de Janeiro. SBM. 2007.

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

LITOLDO, Beatriz Fernandes; BRITO, Arlete de Jesus. **CRIPTOGRAFIA E SUAS POTENCIALIDADES NA EXPLORAÇÃO DAS IDEIAS ASSOCIADAS À FUNÇÃO AFIM**. In: Annaly Schewtschik (Orgs.). **MATEMÁTICA: ciência e aplicações; v. 3**. Ponta Grossa (PR): Atena Editora, 2019. Disponível em: https://www.atenaeditora.com.br/wp-content/uploads/2019/02/E-book-Matem%C3%A1tica-Ci%C3%AAncia-e-Aplica%C3%A7%C3%B5es-3-1.pdf . Acesso em: 20 de novembro de 2019.

LITOLDO, Beatriz Fernandes; LAZARI, Henrique. Uma análise do uso da criptografia nos livros didáticos de matemática do ensino médio. **REVISTA REMATEC**, Natal (RN), v. 9, n. 17, set. - dez., 2014, p. 135-156. Disponível em: http://www.rematec.net.br/index.php/rematec/issue/view/18/17. Novembro de 2020 Acesso em: 01 de novembro de 2020.

LOUREIRO, Flávio Ornellas. **Tópicos de criptografia para o ensino médio.** 2014. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) - Universidade Estadual do Norte Fluminense Darcy Ribeiro, Campos dos Goytacazes, 2014, 43 p. Disponível em:

http://uenf.br/posgraduacao/matematica/wpcontent/uploads/sites/14/2017/09/29082014Flavio-Ornellas-Loureiro.pdf Acesso em: 26 dez. 2019.

LUDWIG, L.; REBELATTO, M.; DA SILVA, S. O estado da arte das criptografias modernas: uma revisão sistemática da literatura. **Revista Brasileira de Computação Aplicada**, v. 12, n. 2, p. 46-53, 2 jun. 2020.

LUDWIG, Lara; REBELATTO, Miguel Grando; SILVA, Sandro José Ribeiro da. O estado da arte das criptografias modernas: uma revisão sistemática da literatura. **Revista Brasileira de Computação Aplicada – RBCA**, Canoas, RS, Brasil, Vol. 12, Nº 2, p. 46–53, julho de 2020. Disponível em: https://doi.org/10.5335/rbca.v12i2.10455 . Acesso em: 28 de setembro de 2020.

MACHADO, Diego; DONEDA, Danilo. **PROTEÇÃO DE DADOS PESSOAIS E CRIPTOGRAFIA: tecnologias criptográficas entre anonimização e pseudonimização de dados.** In: Danilo Doneda e Diego Machado (coord). **A CRIPTOGRAFIA NO DIREITO DO BRASILEIRO.** São Paulo: Thomson Reuters, 2019. (pp.99-125)

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

MARCACINI, Augusto Tavares Rosa. **Direito e informática: Uma abordagem jurídica sobre criptografia.** Rio de Janeiro: Forense, 2002.

MARTIN, Gilbert. **A Segunda Guerra Mundial: os 2.174 dias que mudaram o mundo**. Tradução Ana Luísa Faria e Miguel Serras Pereira. - 1. ed. - Rio de Janeiro: Casa da Palavra, 2014.

MENDES, Abreu Iran. O Estudo da Realidade como Eixo da Formação Matemática dos Professores de Comunidades Rurais. **Boletim de Educação Matemática**, Rio Claro - SP, v. 23, n. 36, p. 571-595, agosto 2010. Disponível em: https://www.redalyc.org/articulo.oa?id=291221905002 . Acesso em: 01 de novembro de 2020.

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

MOURA, Moisés de Oliveira. **A criptografia motivando o estudo das funções no 9º ano do ensino fundamental.** Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Arraias - Curso de Pós Graduação (Mestrado) Profissional em Matemática. Arraias, TO, 2019. 92 p. Disponível em: http://repositorio.uft.edu.br/handle/11612/1373. Acesso em: 28 de setembro de 2020.

PEREIRA, Nádia Marques Ikeda. **Criptografia: uma nova proposta de ensino de matemática no ciclo básico.** 2015. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista Júlio de Mesquita Filho, Ilha Solteira, 2015. 78 p. Disponível em:

https://repositorio.unesp.br/bitstream/handle/11449/127733/000844677.pdf?sequence=1&isAllowed=y . Acesso em: 28 de setembro de 2020.

PIMENTA, Andréa Lira Ribeiro. **Segurança nos contratos internacionais de compra e venda na Internet: criptografia e assinatura digital.** Programa de Graduação em Relações Internacionais. Monografia: Graduação em Bacharel em Relações Internacionais. Centro Universitário de Brasília – UniCEUB. Brasília, 2004, 59 p.

PRESSMAN, R. S. **Engenharia de software**. 5. ed. Rio de Janeiro: McGraw-Hill, 2002.

PRODANOV, C. C.; FREITAS, E. C. de. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2ª. ed. Novo Hamburgo: Feevale, 2013. 227 p.

RODRIGUES, Luciana Ávila; BATISTA, Leonardo Melo; MOURA JÚNIOR, José Teixeira**. Mat ou morra: uma atividade lúdica envolvendo enigmas matemáticos**. In: CONFERÊNCIA INTERAMERICANA DE EDUCAÇÃO MATEMÁTICA, 15., 2019, Medellín, Colombia. Anais [...]. Medellín, Colombia: Universidad de Medellín; Universidad de Antioquia, 2019. Disponível em: http://ciaemredumate.org/conferencia/index.php/xvciaem/xv/paper/viewFile/761/270 . Acesso em: 09 de agosto de 2020.

ROSSETO, Cintia Kohori. **Criptografia como recurso didático: uma proposta metodológica aos professores de matemática**. Dissertação (mestrado profissional) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas, São José do Rio Preto, 2018, 95 f. : il.

SÁ, Ilydio Pereira de. **A magia da matemática – Atividades investigativas, curiosidades e histórias da matemática.** 4ª ed. Rio de Janeiro: Editora Ciência Moderna LTDA., 2018. 178 p.

SAMÁ, Suzi; MOURA, Gabriela Machado; SANTOS, Fernanda Oliveira dos. Ensino de estatística e os nativos digitais: uma proposta para formação inicial de professores**. Caminhos da Educação Matemática em Revista/Online**, v. 9, n. 2, 2019.

SANTANA, Crislaine. **O professor de matemática em início de carreira: desafios e enfrentamentos.** Ouro Preto, 2016. 43 f.: il. Dissertação (Mestrado em Matemática) Produto educacional de educação matemática – Universidade Federal de Ouro Preto, 2016.

SANTOS, Ana Paula Ferreira dos. **A criptografia no ensino fundamental II: contexto histórico, cifras simétricas, aplicações de conteúdos matemáticos e muitas outras curiosidades**. Campos dos Goytacazes, 2016. 130 f.: il. Dissertação (Mestrado em Matemática) Universidade Estadual do Norte Fluminense Darcy Ribeiro. Centro de Ciência e Tecnologia. Laboratório de Ciências Matemáticas. Campos dos Goytacazes, 2016.

SANTOS, José Luiz dos. **A arte de cifrar, criptografar, esconder e salvaguardar como fontes motivadoras para atividades de matemática básica.** 2013. 81f. 2013. Tese de Doutorado. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal da Bahia, Salvador.

SINGH, Simon. **O livro dos códigos: A ciência do sigilo – do antigo Egito à criptografia quântica.** Tradução de Jorge Calife. 10ª Ed. Rio de Janeiro: Record, 2014. 446 p.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas.** Tradução Daniel Vieira; Revisão técnica Paulo Sergio Licciardi Messeder barreto, Rafael Misocki. 6ª Ed. São Paulo: Pearson Education do Brasil, 2015. 562 p.

TEIXEIRA, Tarcisio; SABO, Paulo Henrique, Sabo, Isabela Cristina. WHATSAPP E A CRIPTOGRAFIA PONTO-APONTO: TENDÊNCIA JURÍDICA E O CONFLITO PRIVACIDADE VS. INTERESSE PÚBLICO. **Rev. Fac. Direito UFMG**, Belo Horizonte, n. 71, pp. 607 - 638, jul./dez. 2017. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/view/1882/1784 Acesso em: 30 de novembro de 2019.

VILANUEVA, David Armando Zavatela. **Princípios e análise de exercícios de cálculo.** São Paulo: Editora Livraria da Física, 2014. 285 p.

APÊNDICE A – Questionário usado na coleta de dados da pesquisa

Criptografia para o ensino de funções Afins e suas Inversas

Olá,
Somos acadêmicos do curso de licenciatura em matemática do Instituto Federal do Amapá - IFAP, campus Macapá, Luciana dos Santos Rodrigues e Salomão Lima Monteiro, sob a orientação do professor André Ferreira e Coorientação do professor Eonay Barbosa.

Viemos por meio deste solicitar a partir de sua experiência com a disciplina Matemática, que você possa contribuir com nossa pesquisa, avaliando uma situação didática na qual utilizamos um aplicativo como ferramenta facilitadora em uma aplicação do conteúdo de funções e a utilização da criptografia como motivação.

Sua contribuição consistirá em responder ao questionário a partir de suas experiências e da análise de nossa proposta didática.

Desta forma agradecemos pelo seu empenho em contribuir com a nossa pesquisa.

LINK DA PROPOSTA:
https://drive.google.com/file/d/1gPeYLmc65nJZIwRAJlN9VLdRATTkIKii/view?usp=sharing

LINK DO APP: http://ultratec.link/app/criptodatica/

LINK VÍDEO TUTORIAL:
https://drive.google.com/file/d/1GPq6AYIGcGLCQ0zbTTVTFw0rDxUCNkDv/view?usp=sharing

Endereço de e-mail *

Seu e-mail

1. Em qual instituição você se graduou? *

Sua resposta

2. Ano em que se formou: *

Sua resposta

3. Há quanto tempo atua como professor(a) de matemática? *

- a) Há menos de 1 ano.
- b) Entre 1 e 5 anos.
- c) Entre 6 e 10 anos.
- d) Entre 11 e 15 anos.
- e) Há mais de 15 anos.

4. Entre as modalidades de curso de pós-graduação listadas abaixo, assinale a opção que corresponde ao curso de mais alta titulação que você completou. *

- a) Não fiz ou ainda não completei nenhum curso de pós-graduação.
- b) Especialização (mínimo de 360 horas)
- c) Mestrado
- d) Doutorado

5. Em sua formação acadêmica você teve contato com as componentes curriculares nas quais tenham estudado as TDIC's

- a) Sim
- b) Não

6. Você trabalha ou trabalhou conteúdos matemáticos a partir de um tema gerador? Se sim, exemplifique. *

- a) Sim
- b) Não

6. Exemplifique (Tema X conteúdo).

Sua resposta

7. Em uma escala de 0 a 5, em que nível você consideraria o tema criptografia para ser abordado no ensino de funções? *

- a) 0
- b) 1
- c) 2
- d) 3
- e) 4
- f) 5

8. Em uma escala de 0 a 5, em que nível você costuma buscar novas aplicações dos conteúdos abordados em sala de aula, afim de tornar suas aulas mais dinâmicas? *

- a) 0
- b) 1
- c) 2
- d) 3
- e) 4
- f) 5

9. Em uma escala de 0 a 5, em que nível as técnicas para criptografar mensagens, palavras, frases ou textos através de funções, no seu entendimento, poderiam estimular a aprendizagem? *

- a) 0
- b) 1
- c) 2
- d) 3
- e) 4
- f) 5

10. Em uma escala de 0 a 5, em que nível a utilização do web aplicativo como ferramenta na sua visão poderia contribuir para a realização de atividades mais dinâmicas em sala de aula?

- a) 0
- b) 1
- c) 2
- d) 3
- e) 4
- f) 5

11. Em uma escala de 0 a 5, em que nível você utilizaria este aplicativo como ferramenta em suas aulas?

- a) 0
- b) 1
- c) 2
- d) 3
- e) 4
- f) 5

12. Você conhece ou utiliza softwares e/ou aplicativos voltados para o ensino de funções? Se sim, qual (is)? *

- a) Sim
- b) Não

12. Qual(is).

Sua resposta

13. Deixe aqui algum comentário ou dica para os licenciandos que estão realizando esta pesquisa.

Sua resposta

Enviar

Nunca envie senhas pelo Formulários Google.

ANEXO A - Termo de Consentimento

Declaro que fui informado(a) de que este questionário se refere à pesquisa elaborada pelos acadêmicos Luciana dos Santos Rodrigues e Salomão Lima Monteiro, para preparo de sua Monografia de Conclusão do Curso de Licenciatura em Matemática junto ao Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP, Campus Macapá, pelo que estou datando e assinando este Termo de Consentimento Informado autorizando, inclusive para possível publicação dos resultados deste seu trabalho.

Data:_____/_____/_____

_____.

Assinatura.