UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
***CAMPUS* CHAPECÓ**
PROGRAMA DE MESTRADO PROFISSIONAL EM REDE NACIONAL
PROFMAT

REGINALDO CRISTIANO GRISELI

CRIPTOGRAFIA: UMA PROPOSTA PARA A EDUCAÇÃO BÁSICA

CHAPECÓ
2018

REGINALDO CRISTIANO GRISELI

CRIPTOGRAFIA: UMA PROPOSTA PARA A EDUCAÇÃO BÁSICA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, da Universidade Federal da Fronteira Sul – UFFS como requisito para obtenção do título de Mestre em Matemática sob a orientação da Prof.ª Dra. Janice Teresinha Reichert.

CHAPECÓ
2018

UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

Rodovia SC 484, km 02
CEP: 89801-001
Caixa Postal 181
Bairro Fronteira Sul
Chapecó – SC
Brasil

Griseli, Reginaldo Cristiano
Criptografia : uma proposta para a educação básica / Reginaldo Cristiano Griseli. -- 2018.
105 f. : il.

Orientador: Janice Teresinha Reichert.
Dissertação (Mestrado) -- Universidade Federal da Fronteira Sul, Programa de Pós-Graduação Profissional em Matemática em Rede Nacional, 2018.

1. Matemática. 2. Criptografia. 3. Aritmética . 4. Educação básica . I. Reichert, Janice Teresinha, orient. II. Universidade Federal da Fronteira Sul. III. Título.

Ficha catalográfica elaborada pela
Biblioteca Chapecó – UFFS

REGINALDO CRISTIANO GRISELI

CRIPTOGRAFIA: UMA PROPOSTA PARA A EDUCAÇÃO BÁSICA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal da Fronteira Sul - UFFS, para obtenção do título de Mestre em Matemática.

Orientadora: Prof[a]. Dra. Janice Teresinha Reichert

Aprovado em: 25 / 09 / 18

BANCA EXAMINADORA

Janice T. Reichert

Prof [a]. Dra. Janice Teresinha Reichert - UFFS

Cleonis Viater Figueira

Prof [a]. Dra. Cleonis Viater Figueira - UTFPR

Prof. Dr. Vitor José Petry - UFFS

Chapecó/SC, setembro de 2018

AGRADECIMENTOS

- A Deus, pela existência e capacidade de realizar este trabalho.
- À minha orientadora, professora Janice, por toda ajuda, apoio, auxílio, comprometimento e conhecimento repassados.
- Aos professores do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT - UFFS - pelo conhecimento, contribuições e incentivo durante este processo.
- À Suzana, minha esposa, pelo apoio durante toda elaboração do trabalho, me fazer acreditar que eu conseguiria realizar mais esse objetivo e por estar presente em minha vida.
- A todos os membros da banca, por suas contribuições na avaliação deste trabalho.
- A toda minha família, pela compreensão, apoio e incentivo para que eu pudesse concluir este curso.
- Aos amigos, colegas de curso e de trabalho que de forma direta ou indireta, me incentivaram e apoiaram.
- À Secretaria de Educação do município de Chapecó por oportunizar a realização da oficina, e aos professores de Matemática que participaram com dedicação das atividades propostas.
- À CAPES e a Sociedade Brasileira de Matemática, pela iniciativa, visando a tão necessária melhoria do ensino de Matemática na Educação Básica de nosso país.

RESUMO

O ensino de Matemática apresenta inúmeros desafios, dentre eles, a motivação para aprender conceitos considerados abstratos. Neste sentido, a Criptografia apresenta-se como algo novo e motivador, possibilitando a relação com conceitos da Educação Básica, como números primos e divisibilidade nos números inteiros, pois utiliza estes conceitos para o desenvolvimento de seus algoritimos. Este trabalho teve por objetivo motivar os professores, e por meio deles os alunos, para o estudo da Criptografia relacionando-a com a Aritmética. Buscou-se contribuir na formação dos professores de modo à ajudá-los a estimular a aprendizagem e despertar o interesse dos docentes e alunos pelo conteúdo de aritmética, com o sentido de superar as dificuldades e desafios que o ensino apresenta. A pesquisa aconteceu com o aprofundamento de conceitos matemáticos, o estudo da Criptografia, através de uma abordagem qualitativa resultando em uma oficina que foi aplicada a professores de Matemática da Educação Básica. O autor apresentou através desta oficina algumas ideias de como a Criptografia pode ser introduzida na sala de aula de forma a motivar os alunos para o estudo da Artimética. Os resultados obtidos foram satisfatórios e mostraram a aplicabilidade das atividades em sala de aula.

Palavras-chave: Matemática. Criptografia. Aritmética. Educação Básica.

ABSTRACT

The teaching of mathematics presents numerous challenges, among them, the motivation to learn concepts considered abstract. In this sense, Cryptography presents itself as something new and motivating, allowing the relation with concepts of Basic Education, as prime numbers and divisibility in integers, because it uses these concepts for the development of its algorithms. This work aimed to motivate teachers, and through them students, to the study of Cryptography relating it to Arithmetic. The aim was to contribute to the training of teachers in order to help them stimulate learning and arouse the interest of teachers and students in the content of arithmetic, with the purpose of overcoming the difficulties and challenges that teaching presents. The research happened with the deepening of mathematical concepts, the study of Cryptography, through a qualitative approach resulting in a workshop that was applied to Mathematics teachers of Basic Education. The author presented through this workshop some ideas about how Cryptography can be introduced in the classroom in order to motivate students to study Arithmetic. The results were satisfactory and showed the applicability of the activities in the classroom.

Keywords: Mathematics. Cryptography. Arithmetic. Basic Education.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Com a evolução da humanidade novas tecnologias são incorporadas à vida das pessoas. Vários itens tornam-se indispensáveis, como por exemplo, a informática, tanto no trabalho, como nos meios de comunicação, nas transações bancárias, entre outros. Muitas dessas operações, se não todas, precisam ser sigilosas, e para isso utilizam-se da Criptografia.

Desta forma, a Criptografia está intimamente presente na vida das pessoas, muitas vezes de forma imperceptível, sendo assim, é adequado usá-la como ferramenta motivadora para a aprendizagem da Matemática, despertando nos alunos o prazer em apreender, conhecer e realizar as atividades relacionadas com o ensino básico.

As dificuldades apresentadas pelos alunos na aprendizagem da Matemática decorrem de vários fatores, entre eles pode-se destacar a falta de contextualização do conteúdo abordado. A procura por soluções para amenizar essa situação demanda do professor de Matemática comprometimento, criatividade, persistência, espírito inovador entre outras virtudes.

Considerando o exposto acima, definiu-se para tema deste trabalho Criptografia como motivação para o estudo da Aritmética na Educação Básica e estabelecido o seguinte problema de pesquisa: "Como utilizar a Criptografia para motivar o estudo da Aritmética na Educação Básica?".

Ainda foram elencadas as seguintes questões de pesquisa:

- O que é Criptografia?
- Porque estudar Criptografia?
- Qual é origem da Criptografia?
- O que é e como funciona Criptografia RSA?
- Quais são conteúdos da Matemática da Educação Básica relacionados à Criptografia?
- Como motivar o professor e por meio deste os alunos da Educação Básica na aprendizagem de conceitos como divisibilidade e números primos usando Criptografia?

O objetivo geral proposto é estabelecer uma forma de abordagem que permita apresentar conceitos de Aritmética na Educação Básica relacionados com a Criptografia que motive o

professor e através deste o aluno e que o auxilie na construção do pensamento e do raciocínio lógico.

Para ajudar a elucidar os problemas desta pesquisa foram definidos os seguintes objetivos específicos:

- compreender o conceito de Criptografia e onde ela se aplica;
- entender porque estudar Criptografia;
- conhecer a historicidade da Criptografia;
- aprender o que é e como funciona Criptografia RSA;
- revisar os conceitos básicos de Aritmética como: divisibilidade, máximo divisor comum, mínimo múltiplo comum, números primos, congruência;
- relacionar Criptografia à conteúdos matemáticos aplicados na Educação Básica e incentivar o professor da Educação Básica a redescobrir os conteúdos matemáticos por meio da Criptografia.

É com o intuito de buscar uma forma de cativar o aluno que este trabalho se apresenta, utilizando a criptografia como ferramenta motivadora, relacionando-a com conteúdos de Aritmética que são ensinados do sexto ao nono ano do Ensino Fundamental.

Essa dissertação inicia, no primeiro capítulo, com o resgate bibliográfico de alguns trabalhos que abordam a Aritmética, as dificuldades e desafios do ensino da mesma na Educação Básica e a relação dos números primos com a Criptografia. Também foram elencadas as habilidades da Base Nacional Comum Curricular que devem ser desenvolvidas do sexto ao nono ano do Ensino Fundamental e que podem ser associadas à Criptografia. Ainda foram estudadas a historicidade da Criptografia, alguns conceitos matemáticos necessários para o entendimento da Criptografia, além do detalhamento da Criptografia RSA, de transposição e substituição.

No segundo capítulo, foi apresentada uma sugestão de atividades, com o objetivo de utilizar a Criptografia como motivação na aprendizagem de alguns conceitos da Aritmética na Educação Básica. Essas atividades foram aplicadas em forma de oficina à professores de Matemática da Educação Básica do município de Chapecó/SC, com o propósito de ampliar a abrangência da utilização deste trabalho com os alunos em sala de aula, multiplicando o conhecimento adquirido por esta pesquisa. Por fim, no quarto capítulo, descreveu-se o desenvolvimento da oficina ministrada aos docentes e avaliação dos resultados.

O material didático desenvolvido neste trabalho teve como público inicial os docentes, para posterior utilização em sala de aula com seus alunos. Os professores puderam conhecer e trabalhar com as atividades de modo a verificar a aplicabilidade do material e com isso pode-se verificar as percepções e avaliações dos docentes quanto ao atividades desenvolvidas.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo descreve as motivações do aluno para aprender Aritmética, além de abordar as dificuldades e desafios do ensino da Aritmética na Educação Básica, a relação entre números primos e a Criptografia, aspectos sobre a Base Nacional Comum Curricular e a historicidade da Criptografia. Além disso, aborda alguns conceitos matemáticos necessários para compreensão do tema e por fim, defini a Criptografia Moderna.

2.1 MOTIVAÇÃO PARA APRENDER ARITMÉTICA.

Ensinar Matemática é um desafio que está relacionado à falta de motivação do aluno para aprender alguns conceitos, porém eles podem ser contextualizados para a realidade dos alunos e, assim, contribuir para a motivação e para o seu amadurecimento.

A Aritmética é um exemplo de conceito matemático que pode ser contextualizado no trabalho em sala de aula com os alunos. Nesse contexto, o professor exerce papel fundamental e dele deve partir a postura de buscar contextualizar os conceitos para a realidade na qual o aluno está inserido. Para isso, os professores devem compreender as realidades e levar em conta as situações que os alunos vivenciam fora do ambiente escolar, afinal, as atividades que os alunos fazem mudam constantemente. O ensino da Matemática necessita de um engajamento do educador matemático:

> Ensinar matemática é desenvolver o raciocínio lógico, estimular o pensamento independente, a criatividade e a capacidade de resolver problemas. Nós como educadores matemáticos, devemos procurar alternativas para aumentar a motivação para a aprendizagem, desenvolver a autoconfiança, a organização, concentração, atenção, raciocínio lógico-dedutivo e o senso cooperativo, desenvolvendo a socialização e aumentando as interações do indivíduo com outras pessoas. (SCHLIEMANN et al., 1995, p. 97).

Motivar o aluno a apreender Matemática, mais especificamente Aritmética, demanda esforço, criatividade e a busca de diferentes formas de ensinar que aproximem a Matemática da realidade do aluno. Pereira et al. (2016, p. 3029) afirma que “despertar nos alunos o gosto pela Matemática é uma tarefa exigente para os educadores e professores”.

A Aritmética é a parte da Matemática que estuda operações básicas, necessárias para

compreender os demais conceitos e conteúdos. Para Gimenez e Lins (1997, p. 12) a Aritmética constitui a base da Matemática escolar. Por si só, já constitui um elemento importante na busca por aprendê-la. Além disso, a Aritmética do século XX oferece respostas a problemas teóricos abertos, muito recentes e entre eles a Criptografia, análise numérica, entre outros (GIMENEZ; LINS, 1997, p. 34).

2.2 AS DIFICULDADES E DESAFIOS DO ENSINO DA ARITMÉTICA NA EDUCAÇÃO BÁSICA.

O ensino da Aritmética apresenta desafios a serem superados. Barbosa (2015, p. 5) afirma que as pesquisas mais recentes em Educação Matemática sinalizam a existência de problemas no ensino e na aprendizagem da Aritmética. Embora isto ocorra, se observa um tratamento mecanizado, baseado em exercícios repetitivos e problemas idealizados. Os alunos não têm oportunidade de encontrar variações nos algoritmos que possam ser úteis para o aperfeiçoamento das habilidades de cálculo mental e estimativas.

É imprescindível saber e conhecer conteúdos básicos da Aritmética. Apesar dos avanços tecnológicos, existem muitos desafios para o ensino da Matemática.

> O enorme desenvolvimento da Matemática nas últimas décadas não impediu que crescessem as dificuldades em ensinar os conteúdos matemáticos. Um dos problemas apresentados pelos alunos está em aplicar os conceitos de aritmética, nos tópicos de divisibilidade, máximo divisor comum e congruência com números inteiros. (GROENWALD et al., 2005, p. 35).

A utilização de exercicíos repetitivos, na maioria da vezes, não contribui para o aluno usar os conceitos aritméticos no seu aperfeiçoamento intelectual, dificultando a aplicação desses em situações do seu cotidiano. Uma das formas de suprir essa dificuldade é o desenvolvimento de atividades didáticas, mas:

> Entre os obstáculos encontrados pelos professores de Matemática na transposição didática dos conceitos citados, e que são importantes para o desenvolvimento do pensamento aritmético, podemos destacar a falta de modelos, pois cada problema se resolve de um modo, além disso, é muito raro encontrar atividades didáticas aplicáveis no Ensino Básico. (GROENWALD et al., 2005, p. 35).

O professor de Matemática deve buscar desenvolver atividades que colaborem na transposição das dificulades apresentadas pelos alunos no aprendizado da Aritmética. Groenwald afirma que:

> As atividades didáticas envolvendo a resolução de problemas podem ser desenvolvidas de forma a estimular nos alunos o interesse pela Matemática, aprimorando o raciocínio lógico e ampliando a compreensão dos conceitos básicos para o refinamento do pensamento aritmético, fazendo com que os mesmos desenvolvam a capacidade de manipular conceitos e propriedades de forma clara e objetiva. (GROENWALD et al., 2005, p. 35–36).

A dificuldade da aprendizagem advém, também, da complexidade na compreensão dos conceitos abstratos, pois "[...]a Matemática, de um modo geral, trabalhada na escola, possui um grande estranhamento com a Matemática da rua, da vida do aluno" (GIL et al., 2008, p. 14). Muitos conceitos algébricos trabalhados em sala de aula não refletem a realidade do aluno e consequentemente há uma dificuldade para que tenha uma contextualização de forma a facilitar o aprendizado.

A aprendizagem da Matemática e dos conceitos a ela atrelados transmite a necessidade dos alunos desenvolverem a capacidade de domínio de abstrair e formalizar certas relações ou situações.

> Todo conceito implica existência de regularidades abstraídas da comparação entre as várias situações em que seus elementos estão em jogo. No caso da Matemática a exigência de abstração é muito maior e rigorosa porque supõe desvincular as regularidades de todos os elementos contextuais. Assim, a noção de número ou ideia de quantidade invariável, depende da abstração de todas as propriedades dos elementos enumeráveis, tais como: tamanho dos objetos, forma, cor, disposição no espaço, etc.(TEIXEIRA, 2004, p. 6).

Quando o aluno não está preparado para apropriar-se dos procedimentos e conceitos abstratos, ele não é capaz, muitas vezes, de empregar esse conhecimento na resolução de problemas, isso provoca dificuldade na aprendizagem da Matemática.

> Sem o desenvolvimento do domínio da linguagem necessária à apreensão de conceitos abstratos (e, portanto extremamente dependentes da linguagem que os constrói) nos seus diversos níveis, não pode haver o desenvolvimento do pensamento matemático (também em seus diferentes níveis). (MALTA, 2004, p. 44-45).

E ainda:

> Sabemos que pensar matematicamente exige, desde cedo, um esforço de abstração e formalização o que demanda, por sua vez, desvincular o pensamento de propósitos e intenções imediatas. Ensinar Matemática é fazer ao aluno um convite à abstração. Esse convite, no entanto, parece que só pode ser aceito ou compreendido se o professor adotar algumas precauções. Em outras palavras, o professor precisa ter uma metodologia que possibilite mediações progressivas entre os significados matemáticos e aqueles que o aluno domina. Em síntese podemos dizer que ensinar é negociar significados.(TEIXEIRA, 2004, p. 12).

Para o professor de Matemática, a tarefa de ensinar implica em conseguir fazer o aluno abstrair, estabelecer relações que na maioria das vezes estão distantes do cotidiano do aluno. O docente tem que utilizar mecanismos que levem o aluno a conseguir visualizar essas relações existentes na Matemática presentes nos conceitos utilizados em sala de aula.

Apesar do avanço da Matemática, as dificuldades e os desafios no ensino da Aritmética ainda persistem, pois muitos alunos possuem dificuldade de compreender conceitos que as vezes se apresentam de forma abstrata. Uma das alternativas é a busca de soluções didáticas com a finalidade de estimular o interesse dos educandos na Matemática.

2.3 RELAÇÃO DOS NÚMEROS PRIMOS E A CRIPTOGRAFIA.

A Criptografia (codificação de mensagens) é uma técnica milenar que vem evoluindo com o passar do tempo. Usada para o envio de mensagens desde o início da escrita, hoje as "operações de serviços disponíveis na Internet, movimentações bancárias e outras transações eletrônicas necessitam da Criptografia para comunicação confidencial de dados" (TAMAROZZI, 2001, p. 41).

> A palavra criptografia tem origem grega (kripto = escondido, oculto; grapho = grafia) e define a arte ou ciência de escrever mensagens em códigos, de forma que somente pessoas autorizadas possam decifrá-las. A criptografia é tão antiga quanto a própria escrita; já estava presente no sistema de escrita hieroglífica dos egípcios e os romanos utilizavam códigos secretos para comunicar planos de batalha. (TAMAROZZI, 2001, p. 41).

Porém, a "a Criptografia moderna não existiria sem os números primos" (VIANA, 2017). A codificação se baseia na teoria dos números, conteúdo da Aritmética, abordado no ensino da Matemática.

Viana (2017) descreve um dos principais problemas do ensino da Matemática: "Nós matemáticos estamos habituados a que nos perguntem para que serve o que fazemos, e nem sempre é fácil responder. Fico imaginando um matemático do Egito antigo pedindo financiamento para sua pesquisa sobre números primos". Isso ocorre por que em determinadas situações os conceitos matemáticos são abstratos e parecem não possuir uma aplicabilidade direta.

Muitos conteúdos ensinados na Matemática são difíceis de contextualizar para os alunos, impedindo que o ensino fique mais atrativo para os mesmos. A Criptografia ajuda a responder a pergunta: "para que posso utilizar números primos e Aritmética?"

Os conceitos matemáticos também apresentam uma evolução e novos usos. Terrada

(1988, p. 1) salienta que resultados sobre números primos e congruências, que, durante tanto tempo, tinham sua importância restrita à Teoria dos Números, passaram a representar importância enorme na Criptografia.

Desta forma, os conceitos antes aplicados em determinadas áreas do conhecimento podem apresentar novas abordagens. "Criptografia, ao mesmo tempo que se serve da Teoria dos Números, propiciou um novo impulso ao seu desenvolvimento, acrescentando-lhe, ainda, novas técnicas de abordagem" (TERRADA, 1988, p. 1).

Vive-se um momento de quebra de paradigmas e rupturas de diversos conceitos na sociedade, e isso se reflete também na escola. Além disso os avanços tecnológicos não podem ser deixados de fora da sala de aula, eles devem ser inseridos e contextualizados com as diferentes áreas do conhecimento. "No nível da educação básica, a codificação de mensagens pode oferecer situações motivadoras e atraentes para o estudo de diversos conteúdos programáticos"(JÚNIOR et al., 2015, p. 32). Esta relação entre a Criptografia e números primos, aliando tecnologia e Matemática, mostra que eles estão intimamente ligados.

2.4 BASE NACIONAL COMUM CURRICULAR (BNCC)

A Base Nacional Comum Curricular(BNCC), que é o documento que define os conteúdos e habilidades que serão desenvolvidas na Educação Básica e no Ensino Fundamental pelas escolas do Brasil, aprovada pelo Conselho Nacional de Educação em 15/12/2017, adota entre suas competências gerais:

> Utilizar tecnologias digitais de comunicação e informação de forma crítica, significativa, reflexiva e ética nas diversas práticas do cotidiano (incluindo as escolares) ao se comunicar, acessar e disseminar informações, produzir conhecimentos e resolver problemas. (BRASIL, 2017, p. 18).

A nova base curricular nacional tem como uma das competência gerais o uso de tecnologias para produção de conhecimento. A Criptografia moderna possui como base o uso de tecnologias. Segundo Brasil (2017, p. 223) a Matemática no Ensino Fundamental por meio da articulação de seus diversos campos, entre eles a Aritmética, precisa garantir que os alunos relacionem observações empíricas da realidade a representações matemáticas e as vinculem a conceitos e propriedades, elaborando hipóteses, deduções e conclusões. O objetivo esperado é de que eles desenvolvam a capacidade de identificar oportunidades de utilização da Matemática para resolver problemas, aplicar conceitos, procedimentos e resultados para obter soluções e

interpretá-las segundo os contextos das situações. Ao final do Ensino Fundamental é importante que os alunos mostrem que foram estimulados a deduzir e verificar algumas propriedades a partir de outras.

Ainda segundo Brasil (2017, p. 256–271), a BNCC elenca habilidades que os alunos do Ensino Fundamental do sexto ao novo devem ter, como algumas apresentadas resumidamente na Tabela 1:

Tabela 1: Habilidades elencadas pela BNCC

Ano	Habilidades
Sexto	Classificar números naturais em primos e compostos; Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor;
Sétimo	Resolver e elaborar problemas com números naturais, envolvendo as ideias de múltiplos, divisores e divisibilidade. Resolver e elaborar problemas que envolvam operações com números inteiros.
Oitavo	Efetuar cálculos com potências de expoentes inteiros. Resolver e elaborar problemas de contagem cuja resolução envolva a aplicação do princípio multiplicativo.
Nono	Resolver e elaborar problemas com números reais, inclusive em notação científica, envolvendo diferentes operações. Efetuar cálculos com números reais, inclusive potências com expoentes negativos e fracionários.

Fonte:Brasil,2017.

A possibilidade de associar Criptografia com Aritmética vem ao encontro no que preconiza a BNCC, pois é viável desenvolver conteúdos como a realização de cálculos que envolvam números inteiros e naturais, elaboração de problemas com múltiplos, divisores, entre outros temas, e relacioná-los com a Criptografia.

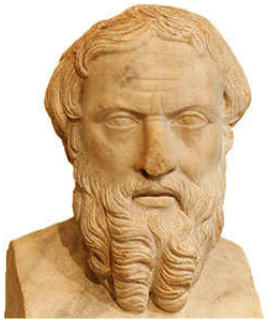
2.5 ORIGENS HISTÓRICAS DA CRIPTOGRAFIA

Nesta seção, realiza-se uma abordagem histórica da Criptografia, mostrando algumas passagens marcantes em sua evolução, para servir de base para que o professor de Matemática e/ou educador possa introduzir esse assunto no ensino básico. A Criptografia esteve presente nas guerras, nos segredos de estados, e continua como um intrumento importante na proteção de informações da internet.

No livro As histórias de Heródoto (485 a.C - 420 a.C), Heródoto, um historiador ro-

mano, narrou um dos primeiros relatos da escrita oculta. Nele são descritos conflitos entre a Grécia e a Pérsia no início do século V a.C. Ele atribui a habilidade da escrita secreta o fracasso do plano de Xerxes (518 a.C - 465 a.C, imperador Persa, de 486 a.C até a data de seu assassinato) invadir a Grécia. Heródoto (Figura 1) relata que Demarato, um grego que foi expulso de sua terra natal, tendo conhecimento dos planos de uma possível invasão de Xerxes, enviou uma mensagem raspando a cera de um par de tabuletas, onde escreveu os planos de Xerxes na madeira e em seguida cobriu novamente com cera, de modo que as tabuletas pareceriam estar em branco, assim sua mensagem chegou aos gregos de forma segura, deixando-os preparados para a invasão (SINGH, 2007, pag. 20).

Figura 1: Busto de Heródoto.



Fonte:https://edukavita.blogspot.com.br/2015/06/biografia-de-herodoto-historiador-grego.html.

Em outro momento da história, em que também ocorreu a utilização da escrita oculta foi a cítala ou bastão de Licurgo (Figura 2) utilizada no século V a.C. pelos espartanos. Eles utilizavam um bastão de madeira, onde era enrolada uma tira de couro ou papiro, no qual era escrita uma mensagem ao longo do comprimento, sendo desenrolada e tranportada como um cinto, com as letras voltadas para o corpo. O mensageiro entregava o código ao destinatário, o qual possuia um bastão idêntico ao do remetente, que conhecia a mensagem ao enrolar a fita (SINGH, 2007, pag. 24). Esse método usado na cítala é chamado de transposição, onde as letras são misturadas formando anagramas.

Figura 2: Cítala

Fonte:https://encriptados.wordpress.com/fotografias/

Outro método usado para o envio de mensagem é o chamado de substituição. Este metodo foi usado por Júlio Cesar (Imperador Romano de 49 a.C a 44 a.C.) e consistia na troca

de cada letra da mensagem original por outra letra do alfabeto, seguindo um padrão. Essa Criptografia foi usada nas Guerras da Gália de Julio Cesar, ficando conhecida como Cifra de Cesar.

Devido a frequência do uso das letras de um determinado idioma, é possível uma pessoa decifrar essa forma de envio de mensagem. Segundo SINGH (2007, pag. 24), a fragilidade dessa forma de Criptografia causou a condenação à morte por decapitação da rainha da Escócia Maria Stuart (1542 - 1587). Ela planejava matar sua prima, a rainha Elizabeth I da Inglaterra, enviando mensagens para seus aliados substituindo letras e algumas palavras recorrentes por símbolos. Mas as mensagens foram interceptadas e decifradas servindo como prova contra a rainha da Escócia.

A cifra de substituição polialfabética consiste em permitir que a mesma letra do texto original fosse codificada de diferentes formas no alfabeto cifrado. Com o exemplo temos o artefato chamado de disco de Alberti, proposto pelo italiano Leon Battista Alberti(1404-1472), considerado como pai da criptologia ocidental, que sugeriu a utilização deste artefato, formado por dois discos de cobre concêntricos distintos, presos por um pino central, com o disco menor móvel sobre o disco maior que ficava fixo. O disco maior continha o alfabeto, em letras maiúsculas, e o menor o alfabeto minúsculo, em ordem aleatória. Ao girar o disco menor, cifrava-se a mensagem. Para a utilização deste sistema, o remetente e o destinatário deviam possuir discos idênticos.

O disco de Alberti serviu de inspiração para construção de máquinas cifradoras. A mais famosa, foi a Enigma (Figura 3), desenvolvida pelo alemão Arthur Scherbius e seu amigo Richard Ritter, para substituir os sistemas de Criptografia inadequados da Primeira Guerra Mundial. Essa máquina foi amplamente utilizada pelos alemães na Segunda Guerra Mundial. Os criptanalistas franceses e ingleses, por aproximadamente treze anos, consideraram as mensagem codificadas por ela indecifráveis. Porém, Alan Turing, um criptoanalista, conseguiu quebrá-la, tendo como inspiração os trabalhos de um jovem matemático polonês chamado Marian Rejewnski. As idéias de Turing serviram de base para construção da máquina Colussus, que quebrou a cifra da máquina Lorenz, uma Enigma aperfeiçoada. A Colussus se tornaria a percursora do computador digital. O uso de chaves simétricas, ou seja, a mesma chave para cifrar e decifrar uma mensagem caracteriza todos esses sistemas.

Figura 3: Enigma.

Fonte:http://www.cryptomuseum.com/crypto/enigma/i/index.htm.

O aumento do uso de computadores e o avanço tecnológico nas décadas seguintes trouxe o desafio da privacidade na troca de informações. Os computadores utilizam códigos binários, e com isso foi preciso transformar todas essas informações nessa linguagem. Essa codificação não é uma cifragem, é apenas tradução à este tipo de linguagem. Para padronizar essas informações foi criado o American Standart Code for Infromation Interchange (ASCHII), que singnifica código padrão americano para o intercâmbio de informação. O próximo passo foi a utilização de sistemas criptográficos padronizados.

Um dos algoritmos de cifragem mais usados era um produto da IBM que foi desenvolvido na década de 70 por Horst Feistel, chamado Lucifer. Uma versão da cifra Lucifer foi oficialmente adotada em 1976 e batizada como Padrão de Cifragem de Dados (DES-Data Encryption Standart) (SINGH, 2001). Esse sistema foi utilizado até 1999, pois como era complexo e operava com uma distribuição de chaves simétricas, resultava em um enorme problema logístico de distribuição de chaves. Hoje são utilizados outros sistemas como o Advanced Encryption Standart (AES) ou o Skipjack.

Devido ao problema da combinação e distribuição de chaves os cientistas Whitfield Diffie e Martin Hellman desenvolveram o conceito de Criptografia de chave pública. Nesta concepção usam-se duas chaves distintas: uma chave chamada de pública e outra chave chamada de secreta (ou privada). A chave pública é usada para cifrar a mensagem enquanto a chave secreta é usada para decifrar a mensagem. (LOUREIRO, 2014). “O mais conhecido dos métodos de Criptografia de chave pública é o RSA. Este código foi inventado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.)[...]”(COUTINHO, 2007).

Como já explanado anteriormente, para entender o funcionamento da Criptografia moderna é necessário o conhecimento de alguns conceitos matemáticos que serão apresentados nas próximas seções, para posteriormente detalharmos a Criptografia moderna.

2.6 CONCEITOS MATEMÁTICOS FUNDAMENTAIS

Nesta seção são apresentados alguns conceitos de Aritmética necessários para a compreensão do funcionamento da Criptografia Moderna, necessários para o entendimento deste trabalho. Os conceitos abaixo baseiam-se em Milies e Coelho (2001, p. 11–185), Hygino (1991, p. 1–268), Coutinho (2014, p. 1–208), Hefez (2014, p. 1–327) onde podem ser encontradas as demonstrações.

2.6.1 Números inteiros

Denota-se o conjunto dos números inteiros da seguinte forma:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

A escolha da letra $\mathbb{Z}$ para representá-lo se dá pelo fato da palavra *Zahl* significar número em alemão. Iniciamente, denota-se o conjuntos dos números inteiros.

Dentro do conjunto dos números inteiros tem-se os conjunto dos números naturais que são representados da seguinte forma:

$$\mathbb{N} = \{0, 1, 2, 3, ...\}$$

O estudo das propriedades dos números inteiros é constatada nas civilizações mais antigas, porém foi na Grécia que primeiramente identifica-se a teoria dos números como a conhecemos hoje.

2.6.2 Divisibilidade

Nesta seção serão abordados alguns conceitos de divisibilidade em $\mathbb{Z}$ necessários para o compreensão deste trabalho.

Definição 2.1 (Divisibilidade)**.** *Dados a e b inteiros, dizemos que a divide b (ou que a é um divisor de b, ou ainda, que a é um múltiplo de b), representando por $a|b$, se existir um $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Quando a não divide b , representamos esse fato por $a \nmid b$.*

Teorema 2.2 (Algoritmo da divisão)**.** *Sejam a e b dois números inteiros com $b \neq 0$. Existem números inteiros q e r, únicos, tais que:*

$$a = b \cdot q + r, \qquad com \qquad 0 \leq r < |b| . \tag{1}$$

Tem-se que q e r são, respectivamente, o quociente e o resto da divisão de a por b. Este é um importante resultado presente na obra Elementos de Euclides que contribuirá neste trabalho.

Demonstração. *Existência:*

Consideramos o conjunto

$$S = \{x = a - b \cdot q; q \in \mathbb{Z}, a - b \cdot q \geq 0\}.$$

Quando $q = 0$, temos que $a - b \cdot q \geq 0$ é um elemento de S, logo, $S \neq \emptyset$.

O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r.

Como $r \in S$, então ele é da forma $r = a - b \cdot q \geq 0$.

Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$.

Por absurdo, suponhamos $r \geq b$. Portanto teríamos que

$$r \geq b,$$

$$r - b \geq 0,$$

$$a - b \cdot q - b \geq 0,$$

$$a - b(q-1) \geq 0,$$

logo, $a - b(q-1)$ também pertenceria a S.

Mas $a - b(q-1) = r - b < r$ (menor elemento), o que é uma contradição

Unicidade:

Suponhamos que $a = b \cdot q + r = b \cdot q' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$.

Assim,

$$0 \leq r < |b| \cdot (-1),$$

$$-|b| < -r \leq 0,$$

$$-|b| < -r \leq 0 \leq r' < |b|,$$

$$-|b| < -r \leq r' - r \leq r' < |b|,$$

logo, $|r'-r| < |b|$.

Por outro lado,

$$b \cdot q + r = b \cdot q' + r',$$

$$b \cdot q - b \cdot q' = r' - r,$$

$$b(q - q') = r' - r,$$

o que implica $|b| \cdot |q - q'| = |r' - r| < |b|$ *o que só é possível se* $q = q'$ *e consequentemente,* $r = r'$.

2.6.3 Máximo divisor comum

Dados dois inteiros a e b, distintos ou não, diz-se que um número inteiro d é chamado de *divisor comum* de a e b se $d|a$ e $d|b$.

Definição 2.3 (Máximo divisor comum)**.** *Seja uma número inteiro* $d \geq 0$. *Diz-se que ele é um máximo divisor comum de a e b, representado por mdc(a,b) se possuir as seguintes propriedades:*

i. d é divisor comum de a e b, ou seja, $d|a$ *e* $d|b$, *e*

ii. d é divisível por todo divisor comum de a e b.

Um dos métodos para determinar o *mdc* de dois números é a decomposição deles em fatores primos, tema que será abordado na próximas seções, porém este método demanda muito trabalho para números grandes. Por isso, é abordado, em seguida, o método de divisões sucessivas, mais conhecido como Algoritmo de Euclides.

Teorema 2.4 (Algoritmo de Euclides)**.** *Sejam dois números inteiros a e b, com* $b \neq 0$, *supondo, então, que* $1 < a < b$ *e que* $a \nmid b$, *então tem-se*

$$a = b \cdot q_1 + r_1, \qquad com \quad 0 < r_1 < b. \tag{2}$$

Ao aplicar o algoritmo de Euclides sucessivamente, tem-se a seguinte sequência

$$\begin{aligned}
a &= b\cdot q_1 + r_1, && com \quad 0 < r_1 < b\\
b &= r_1\cdot q_2 + r_2, && com \quad 0 < r_2 < r_1\\
b &= r_2\cdot q_3 + r_3, && com \quad 0 < r_3 < r_2\\
&\vdots && \vdots\\
r_{n-2} &= r_{n-1}\cdot q_n + r_n, && com \quad 0 < r_n < r_{n-1}\\
r_{n-1} &= r_n\cdot q_{n+1} + 0,
\end{aligned}$$

tem-se algum $r_n | r_{n-1}$, com divisão exata, ou seja, resto igual a 0, sendo que r_n é *mdc* de a e b.

O algoritmo pode ser realizado na prática. Usualmente para efetuarmos a divisão $a = b\cdot q_1 + r_1$ utilizamos o seguinte esquema:

a	b
r_1	q_1

Ao mudarmos um pouco o diagrama temos:

	q_1	
a	b	
r_1		

Ao continuar efetuando a divisão $b = r_1\cdot q_2 + r_2$, sucessivamente, enquanto for possível, teremos

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4	...	r_n	0	

onde r_n é o $mdc(a,b)$.

2.6.4 Mínimo múltiplo comum

Diz-se que um número inteiro é múltiplo comum de dois números inteiros dados se ele é simultaneamente múltiplo de ambos os números. Ou seja, dado a e b inteiros não-nulos, um inteiro c é múltiplo comum de a e b se $a|c$ e $b|c$.

Definição 2.5 (Mínimo múltiplo comum)**.** *Seja uma número inteiro $c \geq 0$. Diz-se que ele é um mínimo múltiplo comum de a e b, indicado por mmc(a,b) se possuir as seguintes propriedades:*

i. c é múltiplo comum de a e b, e

ii. se m é múltiplo comum de a e b, então c|m,

Resumidamente, mmc (a,b) é o menor dentre o múltiplos comum de a e b. A obtenção do mmc(a,b) pode ser efetuado através do seguinte teorema:

Teorema 2.6. *Sejam dois números inteiros a e b, então temos*

$$mmc\,(a,b) = \frac{|a \cdot b|}{mdc\,(a,b)}. \tag{3}$$

A obtenção do mmc também é possível através da fatoração de a e b em números primos, conteúdo que aborda-se-á na próxima seção.

2.6.5 Números primos

Um número inteiro diferente de 0, 1 e -1 que possui somente como divisores positivos 1 e ele próprio é chamado de número primo. Um número inteiro diferente de 0, 1 e -1 que não é primo é chamado de número composto.

Definição 2.7 (Número primo)**.** *Um número inteiro p diz-se primo se tem exatamente dois divisores inteiros positivos, 1 e $|p|$.*

Proposição 2.8 (Lema de Euclides)**.** *Sejam a, b, p $\in$, com p primo. Se p|ab, então p|a ou p|b.*

Demonstração. *Se p|a, a tese está verificada.*

Suponha que p $\not|$a, logo $mdc(p,a) = 1$. Então se $p|a \cdot b$ e $mdc(p,a) = 1$, entã p|b.

O números primos são suficientes para gerar todos os demais números naturais, como afirma o Teorema Fundamental da Aritmética.

Teorema 2.9 (Teorema fundamental da Aritmética)**.** *Todo número natural maior que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como produto de números primos.*

Demonstração. *Usaremos a segunda forma do Príncipio de Indução.*

Se n=2 o teorema é válido, já que 2 é um número primo. Suponhamos o resultado válido para todo número natural menor que n e iremos provar que vale para n. Se n é primo, o resultado está garantido. Se n não é primo, então ele é composto.

Então existem n_1 e n_2 naturais com $1 < n_1 < n$ e $1 < n_2 < n$ tais que $n = n_1 \cdot n_2$. Assim, pela hipótese de indução n_1 e n_2 são primos ou podem ser decompostos em fatores primos, ou seja, $n_1 = p_1 \dots p_r$ e $n_1 = q_1 \cdot \dots q_r$ com p_i e q_i primos, com $i = 1, \dots, r$. Portanto, $n = (p_1 \dots p_r) \cdot (q_1 \cdot \dots q_r)$.

Os números primos, essenciais para a Criptografia RSA, são um grupo infinito. Há 168 números primos entre 1 e 1000, 135 entre 1000 e 2000 e 127 entre 2000 e 3000. Porém com toda a tecnologia computacional atual, ainda há limitações para determinar números primos com várias casas decimais.

Teorema 2.10. *O conjunto dos números primos é infinito.*

Demonstração. *Suponha que o conjuntos dos primos positivos seja finito e sejam $q_1, q_2, ..., q_n$ esses primos. Admita, então, o número $Q = q_1 \cdot q_2 \cdot \dots \cdot q_n + 1$.*

Conforme teorema fundamental da aritmética, Q admite um divisor primo q_i. Como q_i pertence ao conjunto acima, q_i divide o produto $q_1 \cdot q_2 \cdot \dots \cdot q_n$. Então, q_i divide também $1 = Q - q_1 \cdot q_2 \cdot \dots \cdot q_n$, uma contradição.

A distribuição dos primos é bastante irregular e tem sido objeto de estudo de grandes matemáticos. Existem vários teoremas que abordam esse tema, porém sem uma solucão definitiva para números extremamente grandes. A segurança da Criptografia depende da escolha de dois números primos grandes (60 ou mais algarismos cada um). Métodos para encontrar números primos como o Crivo de Erastósteles, primos de Mersenne e primos de Fermat são alguns exemplos. Na próxima seção será abordada a congruência, que tem importante papel na utilização na Criptografia.

2.6.6 Congruências

O conceito de congruência foi introduzido por Karl Friedrich Gauss (1777-1855) em seu livro *Disquisitiones Arithmeticae* de 1801. As notações de congruência presentes no livro são utilizadas até hoje. Gauss escreve em seu livro que foi induzido a usar o símbolo $\equiv$ devido à enorme analogia com a igualdade algébrica.

Definição 2.11. *Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se*

$$a \equiv b \pmod{m}. \tag{4}$$

Considerando-se sempre $m > 1$, a relação $a \equiv b \pmod{m}$ é verdadeira se, e somente se, $m|(a-b)$, ou seja, se existe um inteiro p tal que $a = b + m \cdot p$. Quando a relação não for verdadeira, a e b não são congruentes, ou seja, são incongruentes, módulo m, representados da seguinte forma: $a \not\equiv b \bmod m$.

A definição de congruência é uma relação de equivalência, existindo uma grande semelhança entre as propriedades da congruência e da igualdade, como verificado abaixo.

Um exemplo de congruência que pode ser aplicado em sala de aula, para exemplificar, é o relógio. Este instrumento calcula as horas módulo 12, por exemplo, 16 horas é equivalente à 4 horas, ou seja, $16 \equiv 4\,(mod\ 12)$.

Proposição 2.12. *Seja $m \in \mathbb{N}$. Para todo $a, b, c \in \mathbb{Z}$, tem-se que*

i. $a \equiv b\ (mod\ m)$

ii. *Se* $a \equiv b\ (mod\ m)$, *então* $b \equiv a\ (mod\ m)$

iii. *Se* $a \equiv b\ (mod\ m)$ *e* $b \equiv c\ (mod\ m)$, *então* $a \equiv c\ (mod\ m)$.

iv. *Se* $a \equiv b\ (mod\ m)$ *e* $c \equiv d\ (mod\ m)$, *então* $a + c \equiv b + d\ (mod\ m)$.

v. $a \equiv b\ (mod\ m)$ *se e somente se* $a + c \equiv b + c\ (mod\ m)$.

vi. *Se* $a \equiv b\ (mod\ m)$ *e* $c \equiv d\ (mod\ m)$, *então* $a \cdot c \equiv b \cdot d\ (mod\ m)$.

vii. *Se* $a \equiv b\ (mod\ m)$, *então* $a^n \equiv b^n\ (mod\ m)$ *para todos* $n \in \mathbb{N}$.

viii. $a \cdot c \equiv b \cdot c\ (mod\ m)$ *se e somente se* $a \equiv b\ (mod \frac{m}{mdc(c,m)})$.

Pela divisão euclidiana por m, temos que todo número inteiro é congruente módulo m e, portanto, é congruente a um dos números $0, 1, \ldots, m-1$. Onde podemos chamar de sistema completo de resíduos módulo m a todo conjunto de números inteiros cujos restos pela divisão por m são os números $0, 1, \ldots, m-1$, sem repetição e numa ordem qualquer.

Um sistema reduzido de resíduos módulo m é o conjunto dos números inteiros $r_1, r_2, \ldots, r_{m-1}$, tais que cada elemento do conjunto é primo com m, e se $i \neq j$, então $r_i \not\equiv r_j\,(mod\, m)$. Resumidamente, basta retirar os elementos do sistema completo de resíduos módulo m que não são primos com m para obter um sistema reduzido de resíduos módulo m.

E é a partir dos conceitos de congruêcia que a Criptografia aborda as chaves necessárias para sua segurança, dentre eles alguns teoremas importantes.

Definição 2.13. *Sejam a, p números inteiros, com* $p > 1$. *A congruência* $a \cdot X \equiv 1 \,(mod\, m)$ *possui solução se, e somente se, mdc(a,p)=1. Além disso temos que, se* $x_0 \in \mathbb{Z}$ *é uma solução, então x é uma solução da congruência se, e somente se,* $x \equiv x_0 \,(mod\, m)$.

Proposição 2.14 (Inverso multiplicativo)**.** *Se* $(a,m) = 1$, *então a congruência* $a \cdot X \equiv 1 \,(mod\, m)$ *possui única solução módulo m.*

A proposição acima nos apresenta o chamado inverso multiplicativo, necessário para a decodificação da Criptografia RSA.

2.6.7 Teorema de Euler

O Teorema de Euler do suiço Leonhard Euler, nascido em 1707, é uma generalização do Pequeno Teorema de Fermat.

Definição 2.15. *Chamamos de* $\varphi(m)$ *o número de elementos de um sistema reduzido de resíduos módulo* $m > 1$, *que corresponda ao números de inteiros positivos entre* 0 *e* $m-1$ *que são primos com m, isso define a função* φ *de Euler. Temos que* $\varphi(m) = m-1$ *apenas se m for um número primo, senão* $\varphi(m) < m-1$.

Teorema 2.16 (Teorema de Euler)**.** *Sejam a e m inteiros com* $m > 1$ *e mdc(a,m)=1. Então,*

$$a^{\varphi(m)} \equiv 1 \,(mod\, m). \tag{5}$$

Demonstração. *Sejam* $r_1, \ldots, r_{\varphi(m)}$ *um sistema reduzido de resíduos módulo m, e como mdc-(a,m) =1 temos que* $a \cdot r_1, \ldots, a \cdot r_{\varphi(m)}$ *formam um sistema reduzido módulo m. Logo,*

$$a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdots r_{\varphi(m)} = (a \cdot r_1) \cdot (a \cdot r_2) \cdots a \cdot r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \,(mod\, m),$$

ou seja,

$$a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdots r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \,(mod\, m)$$

e como o $mdc(r_1 \cdot r_2 \cdots r_{\varphi(m)}, m) = 1$, *segue da Proposição 2.12(viii) que podemos cancelar* $r_1 \cdot r_2 \cdots r_{\varphi(m)}$ *de ambos os lados e, portanto*

$$a^{\varphi(m)} \equiv 1 \,(mod\, m).$$

Abaixo é apresentada uma pequena variação do Teorema de Euler, no qual a Criptografia RSA baseia-se:

Proposição 2.17. *Seja m um inteiro livre de quadrados, então para todo $a \in \mathbb{Z}$ e todo $k \in \mathbb{N}$ tem-se que $a^{k\cdot\varphi(m)+1} \equiv a\,(mod\,m)$.*

Um número é dito *livre de quadrados* se não for divisível pelo quadrado de nenhum número diferente de 1.

Demonstração. *Escrevamos $m = p_1 \dots p_r$, onde $p_1, \dots, p_r$ são primos distintos. Como $\varphi(m) = \varphi(p_1)\dots\varphi(p_r) = (p_1-1)\dots(p_r-1)$, pondo $k_i = k(p_1-1)\dots(p_{i-1}-1)\cdot(p_{i+1}-1)\dots(p_r-1)$, tem-se para todo $a \in \mathbb{Z}$, todo $k \in \mathbb{N}$ e todo $i = 1, \dots, r$, que*

$$a^{k\cdot\varphi(m)+1} = a^{k_i\cdot(p_1-1)+1} \equiv a\,(mod\,p_i).$$

2.6.8 Teorema de Fermat

Fermat, numa carta enviada para Bernhard Frénicle de Bessy em 1640, anunciava um resultado surpreendente, que viria a ser conhecido como Pequeno Teorema de Fermat, porém sem a demonstração, sendo que a primeira demonstração foi publicada apenas em 1736, por Euler, quase um século depois.

Teorema 2.18 (Pequeno Teorema de Fermat)**.** *Sejam a um número inteiro e p um primo tal mdc(a,p)=1. Então,*

$$a^{(p-1)} \equiv 1\,(mod\,p). \tag{6}$$

Demonstração. *Note que ao multiplicarmos a congruência $a^{(p-1)} \equiv 1\,(mod\,p)$ por a obtemos $a^{(p)} \equiv a\,(mod\,p)$, ou seja, $a^{(p)} - a \equiv 0\,(mod\,p)$, que é $a(a^{(p-1)}-1) \equiv 0\,(mod\,p)$. Se $mdc(a,p) \neq 1$, temos que $p|a$, e consequentemente, $p|a^p - a$ e, portanto $a^p \equiv a\,(mod\,p)$. Se $mdc(a,p) = 1$, o resultado segue do Teorema de Euler.*

Note que o Pequeno Teorema de Fermat é uma caso particular do Teorema de Euler, pois se p é primo, então $\varphi(p) = (p-1)$.

2.6.9 Métodos para encontrar primos

Como já mencionado antes, a distribuição dos primos é extremamente irregular e tem sido objeto de estudo de grandes matemáticos. O maior primo conhecido foi descoberto por Jo-

nathan Pace em dezembro de 2017 através de um programa de voluntariado que tem como finalidade encontrar números primos de Mersenne chamado GIMPS(Great Internet Mersenne Prime Search). O número descoberto por Pace é um número de Mersenne, chamado de "M77232917" cujo número é $2^{77.232.917} - 1$, composto por 23.249.425 dígitos (CALDWELL, 2017) . Abaixo abordaremos alguns exemplos de métodos, entre eles o de Mersenne, para encontrar números primos.

2.6.9.1 Crivo de Erastóstenes

O Crivo de Erastóstenes é o um dos métodos mais antigos para encontrar os números primos, criado pelo matemático grego Erastóstenes de Cirene, que nasceu por volta de 284 a.C. Esse método não envolve nenhuma fórmula explícita.

O crivo é uma espécie de Peneira. Por volta de 100 d.C. Nicômaco em sua *Aritmética* introduz o crivo da seguinte maneira:

> O método para obtê-los [os números primos] é chamado por Erastóstenes uma peneira, por que tomamos os números ímpares misturados de maneira indiscriminada e, por este método. como fosse pelo uso de um instrumento ou peneira, separamos os primos ou indecomponíveis dos secundários ou compostos. (COUTINHO, 2014, p. 62).

Ao usar o crivo, primeiramente elabora-se uma tabela de todos os números inteiros menores ou iguas a n. Depois, suprimi-se(risca-se) todos números compostos da tabela. Suprima todos os múltiplos de 2, exceto o próprio 2, depois todos os múltiplos 3 diferentes de 3 e assim sucessivamente até o procedimento chegar ao número n.

O procedimento pode ser simplificado, usando o seguinte resultado:

Proposição 2.19. *Se um número natural $n > 1$ não é divisivel por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.*

Demonstração. *Suponha, por absurdo, que n não seja divível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Seja m o menor número primo que divide n; então, $n = m \cdot n_1$, com $m \leq n_1$. Segue daí que $m^2 \leq m \cdot n_1 = n$. Logo, n é divisível por um número primo q tal que $m^2 \leq n$, o que é um absurdo.*

Para n=100 o Crivo de Erastóstenes é o seguinte:

Note que, usando a Proposiçao 2.19, basta riscar os múltiplos dos primos 2, 3, 5 e 7, pois $\sqrt{100} = 10$. Logo, para comprovar se um número n é primo, basta testar que não seja divisível por nenhum primo q que não supere $\sqrt{n}$.

Tabela 2: Crivo de Erastóstene para n=100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Fonte:Autor.

2.6.9.2 Primos de Fermat

Em uma carta em 1640, Fermat enumerou para Frenicle, outro matemático, que os números da forma $F(n) = 2^{2^n} + 1$, para n inteiros entre 0 e 6 eram primos. Os números eram 3, 5, 17, 257, 65.537, 4.294.967.297 e 18.466.744.073.709.551.617. Porém, Euler em 1732 demontrou que $F(5)$ é composto, desmentindo a afirmação de Fermat. O caso $F(6)$ também se verificou, mais tarde, que é composto, restando apenas os cinco primeiros números como primos, conhecidos como Primos de Fermat. Até hoje não se sabe se existem números $F(n)$ primo com $n \geq 5$.

2.6.9.3 Primos de Mersenne

Marin Mersenne, um frade e matemático amador do século XVII, afirmou que são primos os números da forma $M(n) = 2^n - 1$, quando p é um número primo, e por isso receberam o nome de números de Mersenne. É um problema ainda não totalmente resolvido decidir quais números de Mersenne são primos. Sendo que mais recentemente foram encontrados alguns primos de Mersenne através de computadores, entre eles o maior primo já encontrado, já mencionado neste trabalho, além de alguns casos particulares, como para os valores de p no intervalo de $2 \leq p \leq 5000$ que correspondem à: 2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1.279, 2.203, 2.281, 3.217, 4.253 e 4.423.

Além destes métodos existem outros para a descoberta de números primos, porém é através dos números de Mersenne e o uso de computadores que estão sendo encontrados os maiores números primos já conhecidos. Como vimos, o conjunto dos números primos é infinito,

porém existe a dificuldade em descobrir como os primos se distribuem, qual a velocidade de crescimento. Uma maneira é usar o famoso Teorema dos Números Primos cujo enunciado é

$$lim_{x\to\infty}\frac{\pi(x)\cdot\log x}{x}=1, \tag{8}$$

que foi conjeturado por Gauss e Legendre no século passado, mas apenas em 1896 foi provado por Hadamard e Vallé-Poussin de forma independente, onde $\pi(x)$ é o número de primos positivos menores que um dado número real x.

Os números primos estão diretamente ligados a Criptografia, determinar se um número é primo é mais fácil do que tentar fatorá-lo. É neste ponto que a Criptografia baseia-se.

2.7 CRIPTOGRAFIA

"Em grego, *cryptos* significa secreto, oculto. A Criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la." (COUTINHO, 2014, p. 1). Conforme visto no capítulo 2, a Criptografia é usada desde antigamente, evoluindo com o passar do tempo e incorporando as novas tecnologias onde o sigilo das informações transmitidas via internet é realizada através do uso da Criptografia.

Como os computadores utilizam códigos binários, foi necessário primeiramente padronizar a transformação de todas as informações neste código. Por isto foi criadao o American Standard Code for Information Interchange (ASCII), que significa o Código Padrão Americano para o Intercâmbio de Informações, onde ele traduz os símbolos (letras, números...) para a linguagem binária, sendo que esse código não é uma forma de Criptografia (HEFEZ, 2014, p. 316).

Na cripotografia moderna, para atender as demandas das novas teconologias, foi necessário criar novos códigos, que fossem difíceis de decifrar, mesmo com a ajuda de computadores. Esses códigos modernos são chamados de chave pública, onde a utilização de um código de chave pública implica que saber codificar não pressupõe em saber decodificar (COUTINHO, 2014, p. 3).

Um dos problemas na troca das chaves públicas ou senhas era o "[...]paradigma da impossibilidade da troca de senhas sem a intermediação de um portador. Coube a três norte-americanos, Whitfield Driffie, Martin Helmann e Ralph Merkle, quebrar esse paradigma" (HEFEZ, 2014, p. 317). Eles começaram a usar a Teoria dos Números através da noção de congruências para resolver esse problema.

A seguir é descrita a ideia elaborada:

> João e Maria querem trocar entre si uma chave secreta por meio de uma comunicação insegura, como, por exemplo, o telefone.
>
> Eles escolhem em comum acordo um par de números naturais a e m e os tornam públicos. João escolhe um outro número natural α_J e mantém secreto. Com ele, calcula o único número $\beta_J < m$ tal que $\alpha^{\alpha_J} \equiv \beta_J \mod m$, e o envia para Maria. Por sua vez, Maria escolhe um número natural α_M, mantendo-o secreto, e com ele calcula o único número $\beta_M < m$ tal que $\alpha^{\alpha_M} \equiv \beta_M \mod m$, e o envia para João.
>
> Em seguida, João calcula $\beta_M^{\alpha_J}$, obtendo,
>
> $$\beta_M^{\alpha_J} \equiv (\alpha^{\alpha_M})^{\alpha_J} \equiv \alpha^{\alpha_M \alpha_J} \equiv \alpha \mod m, \quad \text{com} \quad \alpha < m$$
>
> Por sua vez, Maria calcula $\beta_J^{\alpha_M}$, obtendo,
>
> $$\beta_J^{\alpha_M} \equiv (\alpha^{\alpha_J})^{\alpha_M} \equiv \alpha^{\alpha_J \alpha_M} \equiv \alpha \mod m, \quad \text{com} \quad \alpha < m$$
>
> (HEFEZ, 2014, p. 317–318)

João e Maria trocaram a chave secreta, onde são públicas as informações a, m, β_J e β_M e secretas o α_J, que somente João conhece, α_M, que somente Maria conhece, e α, que apenas ambos conhecem. O sucesso desse método está na dificuldade de descobrir β_M, α_J e α, o qual foi denominado de DHM, em homenagem aos seu inventores. Porém esse método funciona apenas para a troca de chaves entre dois indivíduos de cada vez, insatisfatório para o mundo que vivemos. Esse método é conhecido como chaves simétricas.

No sistema de chaves simétricas a mesma chave é usada para cifrar e decifrar uma dada mensagem, já nos sistema de chaves assimétricas, cada ususário teria duas chaves, sendo uma pública para cifragem e outra chave privada para decifrar as mensagens (HEFEZ, 2014, p. 316-319).

Alguns tipos de Criptografia simétrica são: AES, DES, 3DES, IDEA, Blowfish, Two-fish, RC2 e CAST.

AES (Advanced Encryption Standard) é uma cifra de bloco desenvolvido pelo *National Institute of Standards and Technology* (NIST) em 2003 a partir de um concurso que escolheu um algoritmo de chave simétrica para proteger informações do governo federal, e foi adotado como padrão pelo governo dos Estados Unidos, substiuindo o padrão DES, sendo um dos algoritmos mais populares, desde 2006. (OLIVEIRA, 2012, p. 21–24).

A Criptografia tipo DES (Data Encryption Standard) foi o algoritmo mais utilizado no mundo até a padronização do AES. Criado em 1977, pela IBM, permitindo cerca de 72 quadrilhões de combinações, que em 1997 foi quebrado por ”força bruta”em um desafio lançado na

internet. Após isso o NIST passou então a recomendar o 3DES. O 3DES utiliza trê ciframentos sucessivos, sendo uma simples variação do DES, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém para ser um algoritmo padrão ele é muito lento (OLIVEIRA, 2012, p. 21–24).

O algoritmo International Data Encryption Algorithm (IDEA) foi criado em 1991. Ele segue as mesmas linhas gerais do DES. Mas uma implementação pelo IDEA é mais rápida do que uma realizada pelo DES. Sua principal utilização é no mercado financeiro e no programa para criptografia de e-mail pessoal mais disseminado no mundo (PGP). O algoritmo Blowfish foi desenvolvido por Bruce Schneier, que oferece a escolha, entre desempenho ou maior segurança por meio de chaves de tamanho variável. É uma aperfeição do Twofish. Twofish é um algoritmo de uso livre para utilização sem restrição, pois não foi patenteado. Ele utiliza chaves de tamanhos variáveis, realizando 16 interações durante a Criptografia, sendo um algoritmo bastante veloz e uma das poucas cifras incluídas no OpenPGP (OLIVEIRA, 2012, p. 21–24).

O RC2 Projetado por Ron Rivest é voltado para Criptografia de e-mail corporativo, sendo sua chave de tamanho variável. Já o CAST foi criado em 1996 por Carlisle Adams e Stafford Tavares, sendo um algoritmo de cifra de bloco, sendo criado em 1996 O CAST-128 é um algoritmo de Feistel (OLIVEIRA, 2012, p. 21–24).

Para resolver o problema das trocas das chaves simétricas foi desenvolvido o sistema de chaves assimétricas, entre elas temos a RSA, ElGamal, DiffieHellman e Curvas Elípticas, posteriormente detalhadas. Neste sistema existem duas chaves, uma delas é secreta, também chamada de chave privada, e a outra delas sendo pública.

O RSA, atualmente, é o algoritmo de chave pública mais utilizado no mundo, sendo uma das mais poderosas formas de Criptografia de chave pública conhecidas até o momento. Criado em 1977 no MIT, seu nome é composto pelas iniciais de seus inventores: Ron Rivest, Adi Shamir e Len Adleman. Ele se utiliza dos números primos para gerar os códigos (OLIVEIRA, 2012, p. 21–24).

O ElGamal envolve a manipulação Matemática de grandes quantidades numéricas, baseando-se no problema do logaritmo discreto. Obtendo sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração. Já o DiffieHellman é o criptosistema de chave pública mais antigo ainda em uso, sendo outro algoritmo que baseia-se no problema do logaritmo discreto. Os autores deste criptosistema introduziram o conceito de chave pública em 1976. Porém, ele não permite assinatura digital nem ciframento (OLIVEIRA, 2012, p. 21–24).

> Curvas Elípticas - Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie-Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública, o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA. (OLIVEIRA, 2012, p. 21–24)

Como vimos na descrição dos tipos de Criptografia, a RSA é o método mais utilizado atualmente. Por isso, a RSA será detalhado, além das criptografias de transposição e de substituição que possuem chaves simétricas .

2.7.1 Criptografia de transposição

Na Criptografia de transposição as letras são misturadas formando anagramas, onde cada letra conserva sua identidade, apenas muda de posição na mensagem. Contudo "[...] as letras não podem ser misturadas ao acaso, senão, nem mesmo o destinatário, que deveria compreender a mensagem, conseguirá decifrá-la. Assim, o padrão do rearranjo das letras deve ser algo previamente combinado" (SILVA, 2016, p. 12–13).

> Quando utilizamos a criptografia por transposição, a mensagem original é transformada num anagrama. Por exemplo, a palavra SER, pode ser cifrada em 5 (3 - 1) anagramas distintos: RES, RSE, ERS, ESR e SRE. Já a palavra TEORIA pode originar 719 (6 - 1) anagramas diferentes. Se considerarmos a frase: RONALDO REGRESSA AO SPORTING, existem mais de 1,87 x 1020 formas de combinar as letras desta curta frase. (FIARRESGA, 2010, p. 5)

A cítala, forma já descrita anteriormente neste trabalho, é outro exemplo de Criptografia de transposição. Nela, também, os caracteres da mensagem original mudam de posição seguindo um padrão, ou seja, a mensagem é escrita na tira no sentido horizontal do bastão, e ao desenrolar a tira temos a mensagem codificada.

2.7.2 Criptografia de substituição

A Criptografia de substituição consiste em trocar cada letra ou grupos de letras da mensagem original por outra letra do alfabeto, símbolo, figuras ou uma combinação de acordo com padrão predefinido e uma chave.

Esta cifra se divide em monoalfabéticas e polialfabéticas. No primeiro caso o caractere da mensagem original é substituído por outro caractere (letra, símbolo, número, etc) de acordo com uma tabela de substituição pré-definida criando uma relação biunívoca, porém ela apresenta uma fragilidade, pode ser quebrada facilmente pelo análise de frequência das letras do alfabeto. Já na polialfabética cada uma das letras ao longo da mensagem pode ser trocada por diversos caracteres complicando a decodificação da mensagem pela análise de frequência.

2.7.3 Criptografia RSA

A Criptografia RSA foi inventada por Ronald Rivest, Adi Shamir e Leonard Adleman, em 1978, no Laboratório de Ciências da Informação do *Massachusetts Institute of Technolgy* (MIT). É um sistema criptográfico com chaves assimétricas, baseando-se na facilidade de encontrar números primos grandes e ao mesmo tempo na enorme dificuldade prática em fatorar o produto de dois desses números (HEFEZ, 2014, p. 319–320). Este método de Criptografia utiliza-se de propriedades da Teoria dos números, entre elas uma variante do Teorema de Euler.

O sistema funciona da seguinte maneira: primeiramente, escolhe-se dois números primos grandes p e q, mantendo-os em sigilo, e multiplicando-os, obtendo $n = p \cdot q$, sendo n público. O segredo da Criptografia RSA, está neste ponto, temos uma operação fácil de fazer, porém extremamente difícil de fazer sem conhecer p e q.

Para a utilização da Criptografia RSA, primeiramente, é necessário uma pré-codificação, para transformar as letras e símbolos em números, pois nos computadores é usado o código ASCII. Neste trabalho, utilizaremos uma codificação simplificada, conforme Tabela 3 de conversão de letras, para o espaço entre duas palavras utilizamos o número 99 para representá-lo:

Tabela 3: Pré-codificação.

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

Fonte:Autor.

Não é necessário começar pelo número 10, apenas não podemos representar uma letra com apenas um algarismo para não termos ambiguidades, por exemplo, se a letra A fosse representada pelo número 1 e B por 2, o código 21, poderia ser BA ou a letra L.

Para utilizar o RSA, devemos encolher os p e q, que necessariamente devem ser primos. Escolhido p e q, que resulta em n, devemos escolher o $mdc(E, \varphi(n)) = 1$, que garante

que esse número E seja um número inteiro e que seja inversível módulo $\varphi(n)$. Note que, pela Definição 2.15, temos que $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$, pois p e q são números primos. Os números n e E serão a chave pública, onde qualquer pessoa que quiser poderá ter acesso, enquanto os p, q e $\varphi(n)$ são as chaves privadas.

Escolhida a mensagem para ser codificada, esta deve ser pré-codificada, e quebrada em blocos de forma aleatória, tomando-se o cuidado para cada bloco não começar com o número 0 e que o tamanho do mesmo seja menor que o valor n. Cada bloco deve ser codificado separadamente, se atentando de não juntá-los, pois isso torna impossível a decodificação da mensagem.

Para codificar um dos bloco que o denominaremos de a, teremos que calcular o resto da divisão do bloco a elevado ao valor E, ou seja a^E, por n. Esse resto é o bloco codificado, chamado aqui de bloco $C(a)$, que podemos escrever usando congruência da seguinte forma:

$$a^E \equiv C(a) \, (mod \, n),$$

após isso o bloco codificado é enviado para seu destinatário.

O destinatário deverá decodificar, mas antes, deverá calcular o inverso multiplicativo de E que pode ser encontrado usando a Proposição 2.14 que pode ser representada como:

$$E \cdot D \equiv 1 \, (mod \, \varphi(n)),$$

onde D é o inverso procurado.

Estabelecido o inverso D, deve-se calcular o resto divisão de $C(a)^D$ por n obtendo o bloco decodificado, chamado aqui de $B(C(a))$, que pode ser representado da seguinte forma:

$$C(a)^D \equiv B(C(a)) \, (mod \, n).$$

Logo tem-se que o bloco $B(C(a)) = b$ como pretendido, pois existe um $k \in \mathbb{N}$ que $E \cdot D = 1 + k \cdot \varphi(n)$ e pela Proposição 2.17, tem-se que

$$B(C(a)) \equiv C(a)^D \equiv (a^E)^D = a^{E \cdot D} = a^{1+k \cdot \varphi(n)} = a^{1+k \cdot (p-1) \cdot (q-1)} \equiv a \, (mod \, n).$$

O Teorema de Euler, e as escolhas de primos extremamente grandes garante a segurança da Criptografia RSA.

Conhecido o método, apresentamos um exemplo, utilizando números primos pequenos para facilitar os cálculos e o entendimento da Criptografia RSA.

Exemplo. *Para o nosso exemplo utilizaremos p=5 e q=11, logo n=55.*

Assim $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1) = (5-1) \cdot (11-1) = 4 \cdot 10 = 40$*, e portanto* $\varphi(n) = 40$.

Devemos escolher $mdc(E, \varphi(n)) = mdc(E, 40) = 1$*, sendo* $E = 3$*, pois* $mdc(3, 40) = 1$.

A mensagem que será criptografada será "UFFS". A mensagem escolhida após a pré-codificada é representada por "30151528", ou seja, os números correspondentes da mensagem utilizando a Tabela 3, que podemos separar em blocos desse modo: 30-15-1-52-8. Como a divisão dos blocos é aleatória, poderíamos ter dividido de várias maneiras, tomando o cuidado de cada bloco ser menor que 55, e não começar com 0.

Agora,para codificar devemos elevar cada bloco original ao expoente 3 e calcular o resto da divisão desse número por 55, que faremos através das propriedade da congruência, logo temos que:

-bloco 30:

$30^3 \equiv 30^2 \cdot 30 \equiv 20 \cdot 30 = 600 \equiv 50 \,(mod\, 55)$,

-bloco 15:

$15^3 \equiv 15^2 \cdot 15 \equiv 5 \cdot 15 = 75 \equiv 20 \,(mod\, 55)$,

-bloco 1:

$1^3 \equiv 1 \,(mod\, 55)$,

-bloco 52:

$52^3 \equiv 52^2 \cdot 52 \equiv 9 \cdot 52 = 468 \equiv 28 \,(mod\, 55)$,

-bloco 8:

$8^3 \equiv 8^2 \cdot 8 \equiv 9 \cdot 8 = 72 \equiv 17 \,(mod\, 55)$.

Portanto os blocos após codificação ficam da seguinte forma:

$50 - 20 - 1 - 28 - 17$

O destinatário ao receber a mensagem para decoficá-la deve calcular o valor D, através $E \cdot D \equiv 1 \,(mod\, \varphi(n))$*, ou seja,* $3 \cdot D \equiv 1 \,(mod\, 20)$*, portanto se D for 7, temos que* $3 \cdot 7 = 20 + 1$*, logo* $D = 7$.

Para decodificar, devemos elevar cada bloco codificado ao expoente 7 e calcular o resto da divisão desse número por 55, que faremos novamente através de propriedade da con-

gruência, logo temos que:

-bloco 50:

$50^7 \equiv (50^2)^3 \cdot 50 \equiv (25)^3 \cdot 50 \equiv 5 \cdot 50 = 250 \equiv 30\,(mod\,55)$,

-bloco 20:

$20^7 \equiv (20^2)^3 \cdot 20 \equiv (15)^3 \cdot 20 \equiv 20 \cdot 20 = 400 \equiv 15\,(mod\,55)$,

-bloco 1:

$1^7 \equiv 1\,(mod\,55)$,

-bloco 28:

$28^7 \equiv (28^2)^3 \cdot 28 \equiv (14)^3 \cdot 28 \equiv 49 \cdot 28 = 1.372 \equiv 52\,(mod\,55)$,

-bloco 17:

$17^7 \equiv (17^2)^3 \cdot 17 \equiv (14)^3 \cdot 17 \equiv 49 \cdot 17 = 833 \equiv 8\,(mod\,55)$.

Note que ao final da decodificação voltamos a ter os blocos originais, ou seja, "30-15-1-52-8", que ao juntarmos teremos "30151528" e aplicarmos a Tabela 3 teremos "UFFS".

Na Criptografia RSA os valores de p, q e D são a chave privada, e os valores n e E são a chave pública. A segurança deste método reside na dificuldade de se fatorar n quando os valores de p, q são muito grandes, pois os meios de fatoração atualmente disponíveis demandam muito tempo.

A fundamentação teórica mostra que a Criptografia está relacionada com a Matemática, possibilitando o desenvolvimento de materiais didáticos para o ensino. Com isso, nos próximos capítulos, são abordadas as propostas metodógicas deste trabalho utilizando-se desta relação e posterior análise dos resultados com a utilização do materal didático por meio de uma oficina com os professores do Ensino Fundamental.

3 PROPOSTA DE METODOLOGIA PARA INTRODUÇÃO DO TEMA CRIPTOGRAFIA NA EDUCAÇÃO BÁSICA

A pesquisa que envolveu este trabalho foi teórica com aprofundamento dos conteúdos matemáticos. Optou-se pela abordagem qualitativa, pois se deduz que nessa perspectiva é possível uma análise mais minuciosa da situação em questão, o que possibilita conhecer e compreender as circunstâncias particulares em que o objeto do estudo se insere. Além disso, foi realizada uma abordagem qualitativa e quantitativa de modo a descrever à aplicação do produto deste trabalho e sua relação com os participantes.

O trabalho iniciou com uma pesquisa bibliográfica e posterior aplicação em sala de aula, e foi desenvolvido em duas etapas: Na primeira parte, para atender aos objetivos propostos, foi realizado um estudo da relação que existe entre o ensino básico de Matemática e a Criptografia, os conteúdos relacionados presentes na BNCC 2017, com um aprofundamento dos conceitos da Teoria dos Números presentes no Ensino Básico e posterior desenvolvimento de atividades utilizando a Criptografia como recurso didático para aplicação a professores de Matemática do sexto ao nono ano do Ensino Fundamental.

Na segunda etapa, foi realizada uma oficina com professores da rede pública municipal de Chapecó/SC, e poster análise e descrição da participação relativa ao experimento didático: motivação para a realização das atividades; conhecimento teórico necessário, dificuldades e desafios da implementação em sala de aula e perspectiva da utilização desta oficina com os alunos.

O material didático desenvolvido neste trabalho tem por finalidade ser utilizado por alunos de sexto ao nono ano do Ensino Fundamental. No entanto, optou-se por realizar a oficina, primeiramente com os professores, buscando que eles conheçam e desenvolvam as atividades e verificar a aplicabilidade do material, levando-se em consideração as percepções e avaliações dos docentes no desenvolvimento da oficina.

Como já observado, a Criptografia não está presente na BNCC do Ensino Fundamental mas pode ser usada como uma ligação entre o dia-a-dia do aluno e conceitos matemáticos como divisibilidade e números primos fazendo com que o aluno possa verificar a presença constante da Matemática no seu cotidiano, desta forma espera-se contribuir para a formação docente e discente voltada para o ensino básico.

3.1 OFICINA PARA PROFESSORES DE MATEMÁTICA DO ENSINO FUNDAMENTAL

As dificuldades para o ensino da Matemática advém de vários fatores, entre eles a falta de contextualização dos conceitos matemáticos. Uma das formas é tentar estabelecer a relação entre o cotidiano do aluno e os conceitos da Matemática. A Criptografia pode servir para fazer esta relação cativando o aluno na aprendizagem da Matemática ou pelo menos estimulando a buscar o conhecimento a esta ciência.

Desta forma, preparou-se um material constituído de sete atividades abordando Criptografia e conceitos de Artimética. As atividades tem o objetivo de serem de fácil assimilação, utilizando uma linguagem simples, e na medida do possível inserindo conceitos da Artimética para enriquecer o conhecimento dos docentes e alunos visando facilitar o trabalho dos professores e instigar o interesse do aluno pela Matemática.

A sequência das atividades apresenta um aumento gradativo no nível de dificuldade, introduzindo temáticas novas através do uso da História da Criptografia, fazendo conexões entre a Criptografia e conceitos de Matemática, considerando o conhecimento prévio do aluno, estimulando o raciocínio lógico e a aprendizagem. Ao final de cada atividade são apresentadas três perguntas para os participantes responderem sobre a dificuldade, aplicabilidade e quais anos/séries do Ensino Fundamental as atividades podem ser desenvolvidas.

A finalidade da aplicação para um grupo de docentes foi verificar junto a eles a aplicabilidade destas atividade, melhorias e ao mesmo tempo ampliar a quantidade de alunos que podem se usufruir deste material.

A atividade (1) denominada “Cítala (transposição)” (Apêndice C) foi embasada na Criptografia de transposição, com introdução histórica desse tipo de codificação, e confeção de uma cítala caseira com materiais que os alunos possuem (lápis, papel e fita adesiva). Esta atividade não abordou conceitos matemáticos, servindo apenas como introdução para Criptografia e motivação para o aprendizado. Esta atividade teve como referência o trabalho de Santos (2016, p. 61–63).

Na atividade (2) chamada de “Cifra de César (substituição)” (Apêndice D) teve como trabalho de referência Carvalho (2016, p.65–74), a proposta é de elaboração de um dispositivo de encriptação e de descriptação utilizando dois copos descartáveis e duas tiras de papel com as letras do alfabeto fixadas na parte superior dos copos, fundamentando-se na Criptografia por substituição. Esta atividade serviu de base para a próxima tarefa onde relacionamos a Matemática com a Criptografia.

Na prática (3) chamada “Aplicando Matemática relacionada a atividade 2” (Apêndice E) ocorreu a utilização de conceitos aritméticos, como o algoritmo da divisão. Procurou-se estabelecer uma forma de mostrar a Matemática envolvida na Criptografia por substituição por meio de desenvolvimento de tabelas.

Na atividade (4) designada “Congruência” (Apêndice F) houve o aprofundamento da utilização do algoritmo da divisão, com a emprego do relógio para calcular o resto da divisão e a relacionar congruências, conteúdo não utilizado pelos docentes no Ensino Fundamental, mas que pode agilizar as resoluções das atividades envolvendo Criptografia RSA.

A atividade (5) “Codificar usando Criptografia RSA” (Apêndice G), atividade (6) “Decodificar usando Criptografia RSA” (Apêndice H) e atividade (7)“Criptografia RSA(Mensagem)” (Apêndice I) são baseadas na Criptografia RSA. Nelas é apresentado um roteiro utilizando conceitos aritméticos para a codificação e decodificação. Também são expostos alguns conceitos novos como o $\varphi(n)$, mas que na utilização em sala de aula, caso o professor desejar ou julgar pertinente pode ser suprimido.

No início e ao final da prática foi aplicado um questionário (Apêndice B e J) com o objetivo de conhecer os participante, seus pontos de vista quanto a conceitos matemáticos e sua utilização em sala de aula e seus conhecimento sobre Criptografia.

As atividades desenvolvidas foram inseridas neste trabalho na forma de apêndices com o intuito de que o material fosse de fácil acesso para quem quiser utilizar em sala de aula, sem a necessidade de editar o material.

4 RESULTADOS DA OFICINA

A seguir será apresentado um relato da oficina realizada e uma avaliação quanto a participação dos docentes e da aplicabilidade das atividades desenvolvidas. Serão transcritas todas as respostas afim de mostrar os vários pontos de vista dos participantes. As palavras ilegíveis serão substituídas por um asterisco.

4.1 PRIMEIRO ENCONTRO

A oficina sobre Criptografia foi elaborada e aplicada a um grupo de professores de Matemática que atuam no Ensino Fundamental na rede municipal de Chapecó, interior do estado de Santa Catarina, em dois encontros.

O primeiro encontro foi realizado no dia 24 de maio de 2018, e teve duração aproximada de uma hora e quinze minutos, pois as atividades anteriores programadas prologaram-se, utilizando o tempo previsto para esta oficina. Em virtude disso, não foram realizadas todas as atividades programadas para este dia.

A atividade iniciou com a apresentação aos participantes, seguida pela explanação da proposta da oficina, objetivos e demais detalhes, além disso, foi apresentado o programa PROFMAT aos participantes. Em seguida, foi entregue para os participantes o Termo de Consentimento Livre e Esclarecido (TCLE) (Apêndice A) para que os mesmos tomassem conhecimento de como seria desenvolvida a oficina, onde todos assinaram concordando com os termos.

Em um segundo momento foi solicitado aos participantes que respondessem o questionário inicial (Apêndice B) com o intuito de conhecer um pouco dos participantes, seu conhecimento sobre Criptografia e conteúdos de Matemática que seriam utilizados nas atividades desenvolvidas durante a oficina.

Por fim, foi realizada uma revisão de conteúdos matemáticos envolvidos na Criptografia (Mínimo múltiplo comum, máximo divisor comum, algoritmo da divisão, números primos). Durante esta revisão, alguns docentes afirmaram que não usam o algoritmo da divisão no ensino da forma apresentada $(a = b.q + r)$. Dentre os participantes, alguns afirmaram que usam as iniciais dos termos que compõe o algoritmo da divisão para facilitar a compreensão dos alunos. Durante a explanação sobre algoritmo da divisão, alguns discordaram do resto do exemplo da

divisão de (-25) por 4, afirmando que o resto seria (-1), e não 3. Percebeu-se durante a atividade, que alguns docentes não se mostraram muito interessados com a revisão realizada, pois seriam conteúdos conhecidos por eles. Entretanto, observou-se uma ampla participação, o que contribuiu no desenvolvimento da oficina, sendo que um dos participantes me parabenizou ao final do encontro.

A falta de envolvimento de alguns docentes, durante a revisão, decorre, na opinião do autor, pelo fato de antes da apresentação estarem participando de uma atividade de demonstração e prática de jogos para aplicação em sala de aula e a parte introdutória desta oficina é teórica, o que pode ter ocasionado uma desmotivação, ou também pelo fato desses professores conhecerem, ou terem um domínio sobre o conteúdo revisado, não manifestando tanto interesse. A revisão, mesmo não sendo de consenso de todos os participantes, foi muito importante, visto que no questionário inicial, verificou-se uma turma heterogênea, com docentes que possuíam pouco tempo de experiência em sala de aula, enquanto alguns com mais de 30 anos.

O conteúdo que os docentes mais gostaram foi a apresentação das "propriedades dos restos", nomenclatura que foi dada para falar sobre congruência, apesar dos mesmos não usarem estas propriedades na sala de aula. Talvez essa preferência se deu por não usarem esse conceito em sala de aula, segundo o que foi relatado.

Ainda, dentre as atividades realizadas no primeiro encontro, houve a aplicação de um questionário (Apêndice B) com nove perguntas com o objetivo de conhecer os participantes quanto ao conhecimento sobre Criptografia e conteúdos matemáticos. A análise das respostas dos docentes à este questionário sErá detalhado a seguir.

Dos vinte e cinco participantes, nem todos responderam todas as perguntas.

A primeira questão indagoe "Marque qual série você atua no momento, no Ensino Fundamental, e há quanto tempo?", onde todos responderam a está pergunta. A Tabela 4 mostra a quantificação das respostas.

Tabela 4: Respostas da pergunta 01 do questionário inicial.

Ano	Quantidade de docentes	Atua até 1 ano	Atua de 1 a 5 anos	Atua de 5 a 10 anos	Atua a mais de 10 anos
6º ano	22	3	7	7	5
7º ano	19	2	7	6	4
8º ano	21	4	6	7	4
9º ano	18	3	7	5	3
Ensino médio	3	0	1	1	1
EJA	1	0	0	0	1

Fonte:Autor.

Como vários docentes não atuam em apenas um ano, teve-se uma média de vinte docentes trabalhando de sexto ao nono ano do ensino fundamental, e três dos professores lecionando no ensino médio e um no EJA. Verifica-se ainda que a maioria tem entre um e dez anos de docência em cada série, logo, vemos que eles tem uma boa experiência de sala de aula, sendo que alguns possuem experiência docente superior a dez anos. Por outro lado tem-se ainda, alguns com menos de um ano de experiência, compreendendo um grupo com diversas formas e visões de ensinar.

Na segunda pergunta foi solicitado: "Descreva o que você trabalha com cada conteúdo abaixo" para os conteúdos de números inteiros, números primos, divisibilidade, mínimo múltiplo comum e máximo divisor comum, onde obtiveram-se de forma resumida as seguintes formas de trabalho para cada conteúdo:

Números inteiros:*"relação e aplicações do cotidiano, problemas, conceitos, jogos, situações problemas; reta numérica e operações; operações, noção de números positivos e negativos, exercícios; atividades concretas, classificação, 6 operações matemáticas, situações cotidiano, parte lúdica, a partir do conhecimento inicial do aluno, quando utilizar o seu uso, livro, curiosidades, exemplos, tabelas, temperatura, altitude, nível do mar, extrato bancário, número simétrico, módulo, comparações, leitura, situação que se utiliza. Costumam introduzir o conteúdo com situações do dia-a-dia fazendo ligação dos conceitos com o cotidiano. Apresenta a reta numérica (interativa) que costuma usar sempre nas aulas fazendo comparativos, depois uso jogos como o bingo das operações onde exercitem as regras de sinais entre outros (principalmente relacionado ao dinheiro)"*.

Números primos: *"critério de divisibilidade, conceitos, jogos, divisores, os primeiros números primos, conceito, exercícios, exemplos, como descobrir a sua utilização de onde e como, situações do cotidiano, divisores, construção da tabela, livro, crivo, aplicações, número composto e não composto, diferença entre número primo e composto, fatoração, decomposição, Crivo de Erastóstenes, usa a divisão para demonstrar particularidades entre outros".*

Divisibilidade: *"pares, ímpares, primos, conceitos, exercícios, problemas, situações relacionadas com o cotidiano do aluno, os critérios mais importantes, em expressões algébricas, exemplos, atividades concretas, usando contas, problemas com o cotidiano, frações, jogo da divisão, livro, critérios de divisibilidade, aplicações, critérios para 2, 3, 4, 5, 6, 8, 9 e 10, divisão básica, regras dos livros, procura enfatizar a operação de divisão, dando ênfase na exatidão da conta".*

Mínimo múltiplo comum (mmc):" *resolução de problemas, conceitos, exercícios, jogos, situações-problema, exemplos, através do múltiplo e divisor, usa o conceito do livro e comenta com eles sobre algumas regras de divisão, problemas do cotidiano, livros, cálculos, aplicações, fatoração, operação com mmc, demonstração, cálculo com múltiplos, enfatiza a tabuada".*

Máximo divisor comum (mdc):*"resolução de problemas, conceitos, exercícios, jogos, situações problema, exemplos, através do múltiplo e divisor, usa o conceito do livro e comenta com eles sobre algumas regras de divisão, resolução de problemas, livros, cálculos, aplicações, fatoração, operação com mdc, noção, chama atenção deles para a tabuada, onde se encontram."*

Uma das participantes respondeu de uma única maneira para todos os conceitos: *"a partir do conhecimento inicial do aluno, utilizando jogos, cartazes, situações do dia a dia, bem como o conceito de cada conteúdo e atividades relacionadas no primeiro momento atividades sem a situação problema para o atendimento do método da resolução e após atividades relacionando situações-problemas".*

Observa-se que o ensino dos conteúdos matemáticos por esses professores se dá de forma diversificada, e não uniforme, visto a variedade das respostas apresentadas.

Em relação à terceira questão: "Quais dos conceitos abaixo você trabalha com seus alunos? Marque com um X o nível de dificuldade dos alunos de 1 a 5 para assimilar os conceitos, sendo 1 pouca dificuldade e 5 muita dificuldade?" as respostas estão listadas na Tabela 5.

Tabela 5: Conceitos trabalhados pelos docentes em sala de aula.

	Quantidade de docentes que trabalham		**Dificuldade apresentada (Quantidade de respostas para cada grau de dificuldade)**					**Não respondeu o grau de dificuldade**
Conceito	**Sim**	**Não**	**1**	**2**	**3**	**4**	**5**	
Números inteiros:	25	0	2	1	15	6	1	0
Números primos:	22	3	5	9	6	4	0	1
Divisibilidade:	22	3	1	9	6	5	3	1
Mínimo múltiplo comum (mmc):	22	3	0	3	11	5	3	3
Máximo divisor comum (mdc):	18	7	0	4	9	4	3	5

Fonte:Autor.

Verifica-se que a maioria dos docentes trabalham com todos os conceitos, com exceção do máximo divisor comum. Os temas trabalhados apresentam, segundo os professores, um grau de dificuldade na aprendizagem variando de 2 a 4, o que pode ser considerado de média dificuldade.

Na quarta pergunta, foi questionado aos docentes “Qual é sua resposta quando o aluno pede por que estudar número primo?”, obtendo as seguintes respostas:

“Que o número primo tem a característica de ser divisor de apenas dois outros números.”

“Que são importantes para o desenvolvimento de outros conceitos futuros.”

“Ajuda na resolução de problemas.”

“O número primo é muito importante no uso da criptografia, senha de bancos, etc.”

“Diz que será necessário para a aprendizagem posterior.”

“Muito usado no mundo virtual, senhas de seguranças.”

“Para resolver diferentes raízes, decompor os números, para usar notas diferentes no pagamento (Ex.: 10=5+5).”

“Alguns sabem, mas aquele que tem dificuldade de aprendizado tem mais dificuldade para responder.”

"Como eles são base de vários conceitos, é muito utilizado na matemática, impossível trabalhar algo sem eles."

"Pois o estudo dos números primos são uma base para outros conteúdos, onde estes serão muito utilizados."

"Para resolver a decomposição em fatores primos, cálculo do mmc, a operação com frações."

"Para aplicações em conceitos e problemas futuros e atuais."

"Para que ele compreenda a soma de fração usando a decomposição e em outros cálculos."

"É um conceito necessário para os próximos conteúdos. São os números primos que formam qualquer número (o produto deles)."

"Para se saber dividir com facilidade, decompor números e descobrir de que multiplicação se originam, etc."

"Para ajudar a compreender a divisibilidade, o número de divisores."

"Para utilizar nas fatorações, mmc, operações com frações."

"Para aplicar na decomposição de números compostos ao extrair as raízes."

"Para facilitar na fatoração, na extração do mmc."

"Números com dois divisores e uso de cálculos seguintes. Pensamentos, desenvolvimento."

"O número primo facilita a realização de várias situações, por exemplo cálculo de mmc e mdc."

Quatro participantes não responderam esta questão. As respostas apresentam, na sua maioria, a justificativa de estudar números primos devido à necessidade para aprender outros conceitos, para resolver outros problemas matemáticos. Apenas duas das respostas afirmaram que os números primos são necessários na Criptografia, objeto deste trabalho.

Nas respostas verifica-se, ainda, que não existe, uma contextualização do conteúdo aplicado. Usa-se da própria Matemática, para justificar a necessidade do estudo dos números primos.

"Você tem conhecimento sobre criptografia?" foi a quinta questão. Oito docentes afirmaram ter, dezesseis responderam não ter, enquanto uma pessoa respondeu mais ou menos,

sem dar exemplo.

Caso a resposta fosse afirmativo, foi solicitado aos participantes dar exemplo onde ela é utilizada, obtendo os seguintes relatos: *"Proteção de senha de bancos, transações bancárias, comunicação de dados, nas guerras para decifrarem o que os inimigos estão fazendo, nos bancos, senhas, nos números, tabelas, códigos, senha de banco, situação financeiras, códigos"*.

Confirma-se nesta resposta a falta de conhecimento de boa parte dos participantes quanto ao que é Criptografia. Em um dos exemplos, o conceito é confundido, pois o professor afirmou que a Criptografia *"é usada nas guerras para decifrarem o que os inimigos estão fazendo"*, quando na verdade é uma forma de ocultar as informações dos inimigos. Por outro lado, alguns docentes apresentaram exemplos onde a Criptografia é usada realmente, como foi o caso de *"Proteção de senha de bancos, transações bancárias"*.

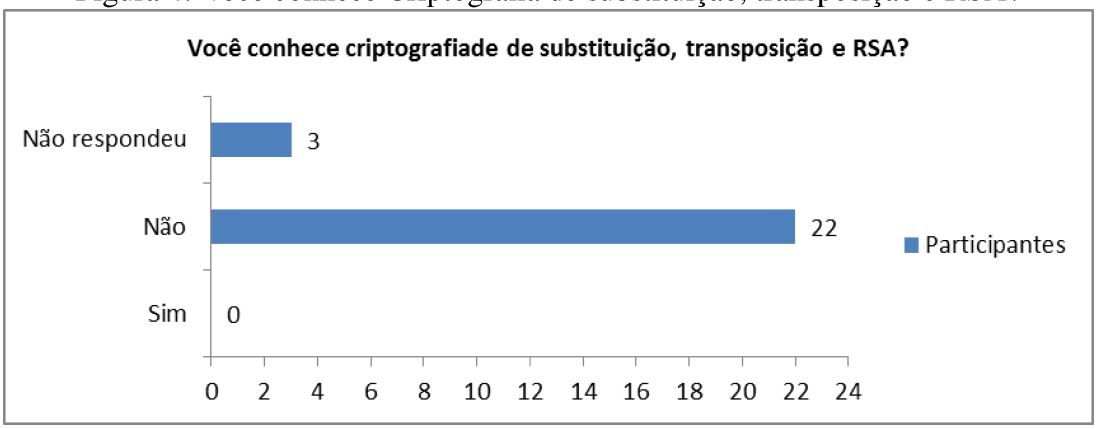
Na questão 6 "Você considera que a Criptografia tem relação com conceitos matemáticos?" dezenove pessoas responderam afirmativo, cinco não responderam, enquanto uma pessoa afirmou que *"pode ter, mas desconheço"*.

Complementando a questão 6, foi questionado (pergunta 7): "Que conceitos matemáticos você considera que sejam utilizados para criptografar códigos?", e obteve-se como respostas: *"Senhas e programação de softwares, números primos, matrizes, arranjo, combinações numéricas, probabilidade, análise combinatória, raciocínio lógico, lógica, deduções, análises, números naturais, combinação e arranjo, desconheço, divisibilidade"*. Nesta pergunta, treze pessoas não responderam.

Aqui recebeu-se diversas respostas, desde *"senhas e programação de softwares"* que não são conceitos matemáticos, até *"números primos"*, tema necessário para a utilização da criptografia RSA.

Na pergunta 8, "Você já tem conhecimento sobre Criptografia de substituição, transposição e RSA?". As respostas são apresentadas no gráfico da Figura 4:

Figura 4: Você conhece Criptografia de substituição, transposição e RSA?

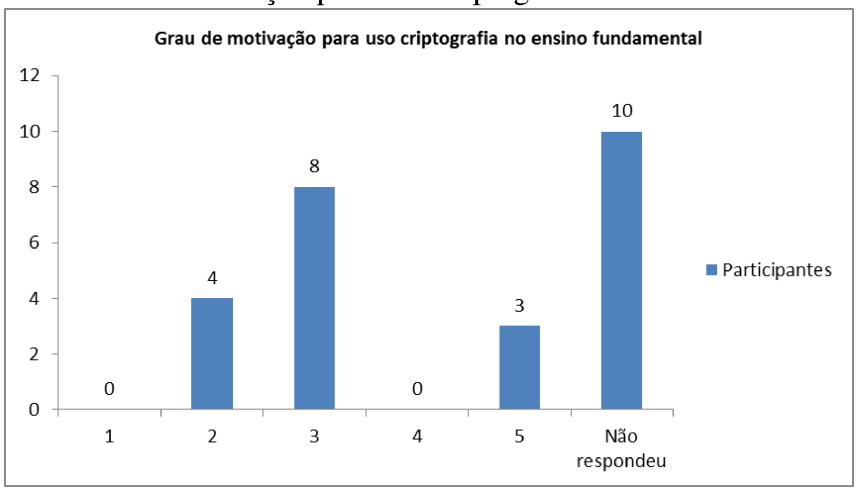


Fonte:Autor.

Aqui verifica-se que a totalidade disse não apresentar conhecimento sobre Criptografia de substituição, transposição e RSA. Nas respostas anteriores, obteve-se exemplos da Cripografia utilizada em bancos, caso da RSA. Logo percebe-se que os participantes não fazem esta relação entre as Criptografias utilizadas nos exemplos dados.

Já na questão 9 "Você considera o tema Criptografia motivador para o ensino de Matemática aos alunos do Ensino Fundamental? Marque 1 para nada motivador e 5 muito motivador.", o gráfico da Figura 5 representa as respostas obtidas.

Figura 5: Grau de motivação para uso Criptografia no Ensino Fundamental.



Fonte:Autor.

Dos quinze docentes que responderam, verifica-se que apenas três, ou seja, 20% acham a Criptografia muito motivadora para o estudo da Matemática no Ensino Fundamental. Isso reflete a falta de conhecimento sobre Criptografia como foi confirmado nas respostas anteriores e como é possível verificar nas justificativas para a resposta da questão 9, que são transcritas em cada nível de motivação a seguir.

Para o nível 2:

"Pouco motivador, pois os alunos nem a tabuada sabem."

"Não conheço o tema."

"Não desenvolvi atividades relacionadas a este tema em sala, de modo que não sei como os alunos iriam se comportar, se saia uma aula interessante ou não."

"Não conheço o tema."

Para o nível 3:

"De certa forma vejo como um conteúdo complicado, e de certa forma inacessível a todos, poucos entenderam."

"Acredito que toda atividade pode trazer alguma ajuda para motivar os alunos."

"Depende de como será abordado e o nível de dificuldade de aprendizagem."

"Despertar o interesse pelo tema."

"Muitas dificuldades de concentração e análises."

"Eu preciso conhecer melhor."

"Deve ser interessante pelo que se vê na mídia."

"Pelo que se pode observar na mídia é um tema bastante presente em filmes que fazem parte da realidade do aluno, pois gostam de assistir. Ao propor o tema criptografia os alunos podem ser desafiados."

Para o nível 5:

"Pois utiliza raciocínio lógico e para os alunos a matemática ficará mais divertida e com mais sentido."

"Instiga o interesse dos mesmos."

"Instiga a curiosidade."

Dos que não responderam o nível de motivação, seguem abaixo as justificativas, dentre estes, quatro não justificaram:

"Ainda não tenho uma opinião formada."

"Preciso conhecer melhor e estudar."

"Não posso opinar, pois desconheço o tema."

"Como não tenho conhecimento não vale marcar."

"Como não tenho conhecimento sobre o tema optei por não responder."

"Por não conhecer o tema, e sua aplicações e relações não é possível observar sua importância no contexto escolar."

É possível constatar pelas considerações feitas pouco conhecimento sobre Criptografia, o que representa um grande desafio para a proposta deste trabalho.

4.2 SEGUNDO ENCONTRO

Nesta segunda parte participaram 31 professores e a coordenadora pedagógica, dentre eles, se fizeram presentes novos participantes que não estavam no primeiro dia, dentre os quais, dois são gestores que atuam eventualmente em sala de aula. Para esses, foi entregue o termo de consentimento e o questionário inicial. Este encontro, que ocorreu no dia 19 de julho, compreendeu todo o turno da manhã, pois na data que seria realizada em junho foi cancelada.

Nesse dia foram desenvolvidas as quatro primeiras atividades, o questionário final (que será analisados abaixo) e uma pequena introdução da quinta atividade. Ao final, os docentes pediram para que as atividades restantes sejam desenvolvidas em data posterior, com dia a ser agendado e que não fará parte da análise deste trabalho.

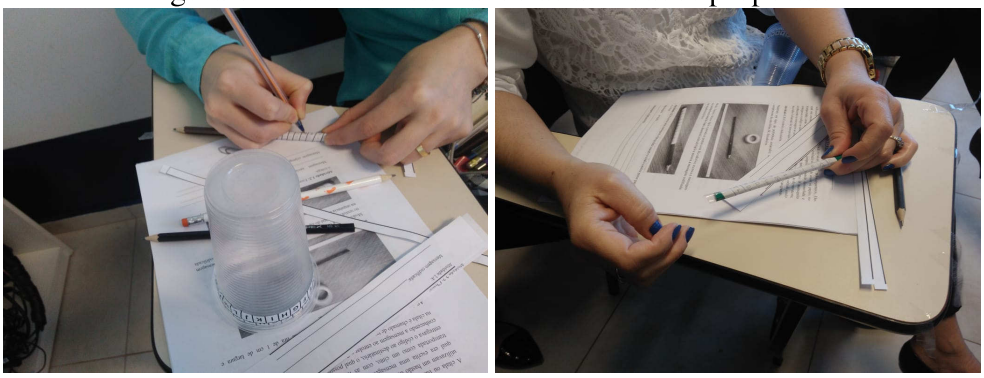
Para o desenvolvimento dessa parte da oficina foram entregues aos participantes as atividades impressas; um kit contendo: Dois lápis hexagonais de tamanhos diferentes, fita adesiva e tiras de papéis para atividade (1); Dois copos descartáveis com uma tira contendo o alfabeto fixada na parte superior do copo e uma tira de papel para troca de mensagem entre eles para atividade (2).

A atividade iniciou com uma dinâmica, onde foi entregue uma "mensagem secreta" a um professor posicionado num lado da sala e solicitado que ele enviasse a mensagem por meio da ajuda dos colegas para outro professor do lado oposto da sala. Durante o trajeto, a mensagem foi interceptada, fazendo referência a um ambiente não seguro para troca de mensagens, situação que pode ocorrer na internet. Em seguida questionou-se qual a forma ou mecanismo que poderia tornar essa troca de mensagens segura de modo que apenas o emissor e o destinatário pudessem ter conhecimento do conteúdo. Com isso, introduziu-se o termo Criptografia, ferramenta que pode tornar essa troca segura e é a base das atividades propostas. Após essa dinâmica procedeu-se com o desenvolvimento das demais atividades.

Todos os docentes participaram da oficina (Figura 6) e realizaram a maioria das ati-

vidades propostas. Durante o desenvolvimento as dúvidas que surgiram foram sanadas entre eles ou através da intervenção do autor. Dentre as sugestões dadas durante a oficina, destaca-se a necessidade de numeração dos copos para realização da atividade (2) de modo a facilitar a execução desta prática.

Figura 6: Docentes realizando as atividades propostas.

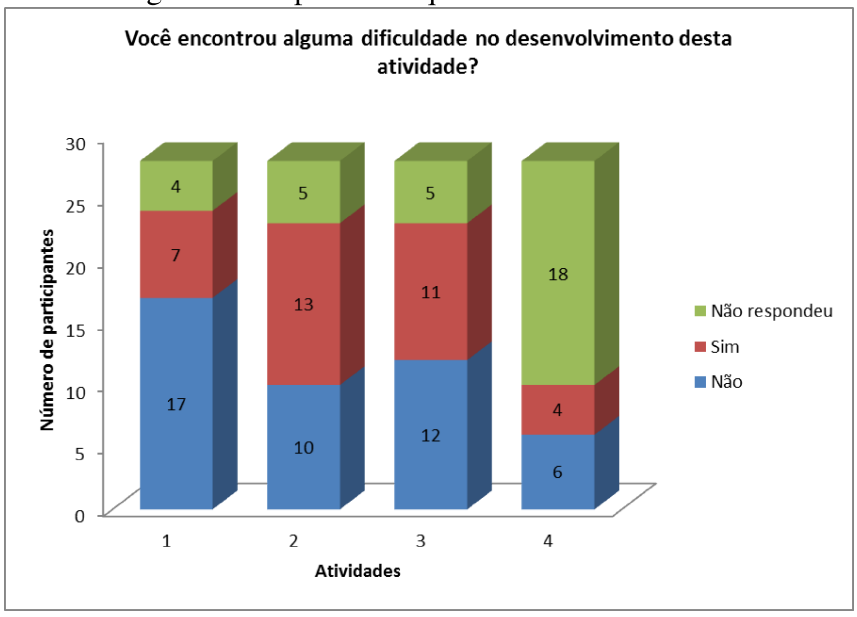


Fonte:Autor.

Ao final de cada atividade foi solicitado aos participantes para responder a três questões que indagavam sobre a dificuldade e a possibilidade do desenvolvimento das atividades com alunos do Ensino Fundamental, sendo que, tivemos poucos participantes respondendo as questões da atividade (4) em vista de ser no final da manhã.

Para a primeira pergunta: "Você encontrou alguma dificuldade no desenvolvimento desta atividade? Qual?", as respostas obtidas são mostradas no gráfico da Figura 7, abaixo.

Figura 7: Respostas da questão 1 das atividades.



Fonte:Autor.

Observa-se que alguns participantes tiveram certa dificuldade, principalmente nas atividades (2), (3) e (4). Com base nos relatos os obstáculos encontrados foram desde falta de borracha no kit, até falta de atenção e concentração, como são relatadas nas respostas obtidas por por atividade:

Atividade 1:

"Sim. Não tínhamos borracha no quite."

"Não, pois a técnica de resolução foi explicada inicialmente."

"Sim, um pouco na colocação das letras nas células."

"Sim, um pouco de atenção."

"Sim, encontrei algumas dificuldades por ser a primeira vez que eu faço este trabalho."

"Não, é fácil a proposta. Porém deveria iniciar as atividades com apenas uma palavra, depois frases..."

"Não, em relação a nos professores, mas em relação aos alunos acho que teriam um pouco de dificuldades."

"Não, foi tranquilo."

"Sim, a falta de concentração e atenção."

"Não encontrei dificuldades."

"No geral não. Porém minha colega errou uma célula, aí dificultou a leitura. Precisou refazer."

"Se não fosse explicado com funções haveria muitas dificuldades."

Atividade 2:

"Um pouco, só até eleger os copos 1 e 2."

"Um pouco."

"Sim, definir e lembrar qual copo é a chave e qual decodifica."

"Sim. Identificar se a letra certa estava em cima ou em baixo. Seguir a mesma ordem."

"Sim. Um pouco."

"Sim, dificuldade de compreender como fazer a mensagem e de entender o que signi-

ficava a chave."

"Um pouco, precisa prestar mais atenção sobre o copo que representa o código e o copo para decodificação. Poderia ter copos com cores diferentes."

"Sim, padronizar quais copos será a mensagem criptografada e qual será o decodificado."

"Demorou um pouco para entender o processo."

"Não, para mim o desenvolvimento foi bem tranquilo."

"Não, achei mais simples."

"Não encontrei."

"Sim. Porque dependendo, se não combina bem qual é o copo da palavra codificada, pode haver confusão."

"Sim. Mas com as explicações ficou claro."

"Mesmo da anterior."

Atividade 3:

"Pouca dificuldade, mais no entendimento inicial."

"No começo sim. Por não ser um hábito, mas depois que a lógica fica clara as atividades ficam mais fácil ou menos complicada."

"Não, só tem que fazer alguns ajustes para os alunos."

"No início de compreender a atividade."

"Algumas dificuldades."

"Um pouco."

"Sim, quando encontramos números negativos a interpretação necessita ser mais complexa."

"Um pouco, no início, depois ficou fácil."

"No copo eu não tinha dificuldade de fazer esta atividade, na tabela eu acho mais difícil."

"Sim, entender os ajustes/divisão da tabela."

"Sim, é fácil fazer confusão."

"Em alguns momentos, precisou mais explicações, mas não é difícil."

Atividade 4:

"Sim, compreender a divisibilidade."

"Foi complicado, mas conseguiria estudar."

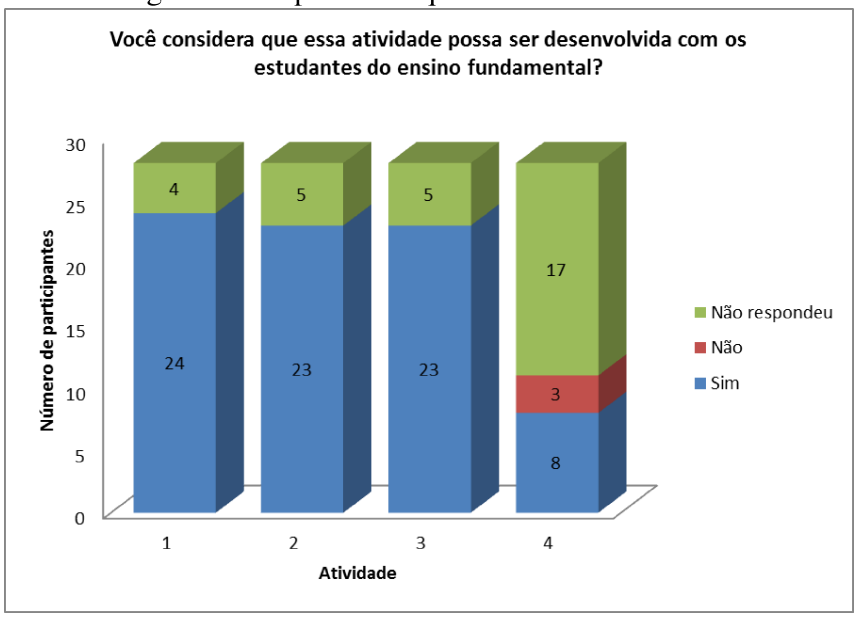
"Um pouco, no momento de somar os meses."

"Um pouco, demorou o entendimento."

Uma das maiores dificuldades verificadas pelos participantes, foi compreender a divisibilidade na forma em que apresentada, através do algoritmo da divisão, pois os professores, em maior número, conforme relatado, utilizam o método da chave. Outra dúvida foi o uso da congruência, que de um modo geral não é trabalhado no dia-a-dia de sala de aula do sexto ao nono ano.

Na segunda questão "Você considera que essa atividade possa ser desenvolvida com os estudantes do Ensino Fundamental?" as respostas são mostradas pelo gráfico da Figura 8:

Figura 8: Respostas da questão 2 das atividades.



Fonte:Autor.

É possível verificar pelo gráfico que, segundo os docentes, as atividades (1), (2) e (3) podem ser trabalhadas no Ensino Fundamental. Alguns ainda sugeriram que devem ser feitas algumas adaptações e averiguado o nível da turma. Com relação à atividade (4), apenas três professores responderam que esta prática não pode ser desenvolvida. A seguir são apresentados considerações referente à esta questão, transcritas por atividade:

Atividade 1:

"Sim. Faz com que unem a criatividade e o conhecimento."

"Sim. Com uma boa explicação prévia eles conseguem fazer sem dificuldade."

"Sim, é ótima para treinar a concentração e atenção."

"Acredito que sim."

"Com algumas turmas sim."

"Sim, bem tranquilo."

"Sim, mas com algumas adaptações."

"Sim. Com turmas de anos finais exemplo 8º e 9º séries."

"Sim, depende do nível de cada turma."

"Pode."

"Sim. Pode ser e eles vão gostar."

"Sim, vão gostar e se interessar."

Atividade 2:

"Sim, mas apenas com alunos maiores, pois exige bastante abstração, seria melhor aplicar no ensino médio."

"Sim, realizava em sala já."

"Sim, depende do nível de cada turma."

"Pode ser desenvolvida."

"Pode ser desenvolvida, porém não em turmas muito grandes."

"Sim, é bem interessante e acho que vão gostar."

"Mesmo da anterior."

Atividade 3:

"Pode sim, mas tem que ser bem explicado no início."

"Penso que sim."

"Sim, da mesma forma que a anterior."

"Sim na do copo é mais fácil para os aluno."

"Acredito que pode ser feita com alunos maiores(8º e 9º ano)."

"Sim. Esta atividade trabalha muito bem o algoritmo da divisão e ao mesmo tempo é divertida."

"Sim, em turmas menores."

"Sim, com turmas mais desenvolvidas e dinâmicas."

Atividade 4:

"Sim, mas é bem complexa."

"Não, acho que não vão entender."

Já na terceira pergunta "Se sim, em qual ano?"obtiveram-se as respostas, que estão compiladas na Tabela 6:

Tabela 6: Respostas da questão 03 das atividades.

	Quantidade de participantes que responderam qual (is) atividade (s) pode(m) ser desenvolvida (s) por série.					
Atividade	**6º ano**	**7º ano**	**8º ano**	**9º ano**	**Ensino Médio**	**Não respondeu**
(1)	13	13	22	21	1	4
(2)	10	11	18	21	1	6
(3)	8	9	20	21	2	6
(4)	3	6	7	7	0	19

Fonte:Autor.

Grande parte dos professores afirmou que as atividades podem ser melhores aproveitadas no 8º e 9º ano, entretanto, alguns docentes responderam que também podem ser utilizadas no 6º e 7º ano. Abaixo se apresentam as considerações feitas pelos professores quanto a essa questão:

Atividade 1:

"Dependendo do nível da turma de 6ºa 9º ano."

"Pode ser trabalhada com aluno de 6º ao 9º ano, cada ano com suas adaptações, respeitando seus limites."

"Em qualquer turma, observando apenas o tamanho da mensagem(sexto ano a mensagem poderá ser mais curta)."

"Penso que a partir do 6º ano, pois os alunos precisam somente compreender que as linhas serão colocadas em colunas."

Atividade 2:

"Devido ao maior raciocínio de quais copos será o padrão, penso ser mais adequado para 8º e 9º ano."

Atividade 3:

"9º ano, talvez 8º com a utilização da tabela."

"A partir do 6ºano, pois quando se trabalha a divisão e o algoritmo, já pode-se introduzir esta criptografia."

Atividade 4:

"A partir do 6º ano, pois utiliza-se somente das 4 operações básicas."

Ao final do encontro foi entregue um questionário com perguntas. Dos participantes apenas vinte e oito pessoas devolveram preenchido, e as respostas obtidas são apresentadas abaixo:

Com relação primeira questão "Você acha que a oficina pode ser aplicada no Ensino Fundamental do 6º ao 9º ano?" 26 professores afirmaram que a oficina pode ser aplicada no Ensino Fundamental, e apenas dois responderam que não pode .

Abaixo são transcritas as justificativas dos participantes que afirmaram que a oficina pode ser aplicada:

"Cativa os alunos a querer mais, sobre a codificação."

"Uma atividade de auxílio nos conteúdos de divisão e multiplicação."

"Só acho melhor muitas funções, conteúdo do 8º e 9º ano."

"Pois são todas adaptações reais."

"Contribui no raciocínio lógico dos alunos, na criatividade."

"Podemos definir o nível de dificuldade (escrever apenas palavras ou uma frase) dependendo do nível da turma."

"Fácil compreensão."

"Atividade simples de fácil compreensão, um pouco de dificuldade com as tabelas."

"Para estimular a divisão."

"Acho que é mais fácil para aplicar na 8º e 9°(transposição) e a do copo."

"Podemos trabalhar com diversos conteúdos e é atrativo aos alunos."

"Para algumas turmas que depende do nível de compreensão matemática."

"Pois é de fácil compreensão."

"Porém apenas com os últimos anos em virtude da abstração que é necessária."

"Algumas atividades parecidas já constam em livros didáticos de matemática."

"Se bem adaptada, pode contribuir na memorização de conteúdos já trabalhados."

"Bem detalhadas elas se tornam atrativas para os educandos."

"Adaptando algumas coisas é possível sim."

"Pois são atividades diferenciadas que despertam interesse dos alunos."

"Possui aplicabilidade e associação com os conteúdos para essas turmas."

"Uma parte da oficina sim, pois é algo novo e a curiosidade em decodificar uma mensagem seria estimulador."

"Em algumas turmas, mas não em todas. Depende do número de alunos, nível da turma."

"Alguns conceitos mais simples os alunos conseguem entender."

Já as pessoas que responderam não ser possível aplicar as atividades, justificaram da seguinte forma:

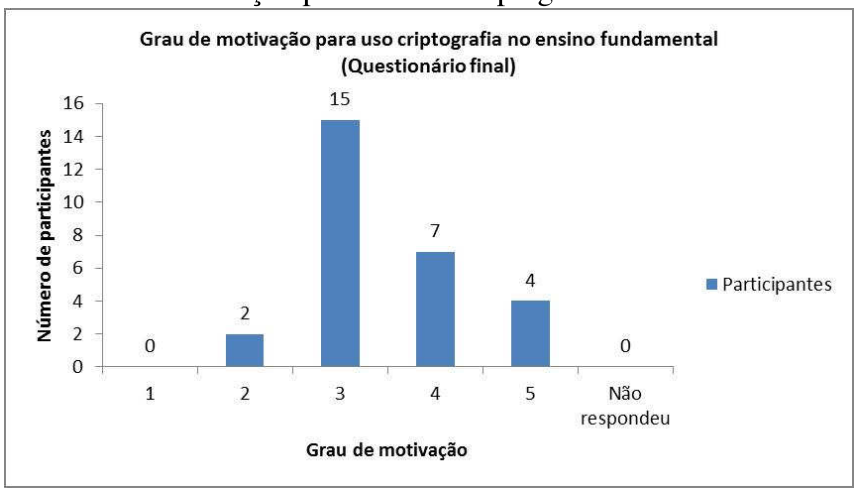
"Algumas dá, outras não."

"Dificuldade para domínio da base."

Observa-se que a maioria dos docentes afirmou que a oficina pode ser aplicada no Ensino Fundamental do 6º ao 9º ano, como foi comprovado nas respostas obtidas em cada atividade. Alguns relatos consideram que o nível da turma e/ou o tamanho da turma pode dificultar a aplicabilidade das atividades, mas de um modo geral, como se pode observar nas justificativas, as práticas propostas podem ajudar a cativar e despertar o interesse no aluno e também contribuir na associação de conteúdos desenvolvidos com as turmas.

Já na questão 2 “Você considera o tema Criptografia motivador para o ensino de matemática aos alunos do Ensino Fundamental? Marque 1 para nada motivador e 5 muito motivador.”, o gráfico da Figura 9 apresenta as respostas obtidas.

Figura 9: Grau de motivação para uso da Criptografia no Ensino Fundamental.



Fonte:Autor.

Dos vinte e oito docentes que responderam esta questão, onze, ou seja, quase 40 % afirmaram que a Criptografia apresenta níveis 4 e 5 de motivação para o estudo de Matemática no Ensino Fundamental. Comparando-se com o gráfico da Figura 5, que apresenta as respostas dessa mesma pergunta realizada no primeiro encontro, quando apenas três participantes responderam os níveis 4 e 5, verifica-se um aumento de mais de 360%. Essa mudança de concepção reflete a contribuição desta oficina, com o conhecimento da Criptografia através das atividades desenvolvidas. Abaixo são transcritas as justificativas, para cada nível de motivação. Vale ressaltar que seis pessoas não justificaram.

Nível 2:

“Para estimular a criatividade do aluno.”

*“Tudo depende do ponto de vista, se abordarem * * alguma coisa sim, mas o coeficiente de divisão é muito complicado para ministrar e o * *.”*

Nível 3:

“Sim, alunos gostam de atividades que saem da rotina.”

“O conteúdo de funções é muito interessante no entanto é o que os alunos tem mais dificuldade.”

“No início vão adorar, mas com o decorrer vão achar repetitivo.”

"Acredito chamar atenção dos alunos. Torna as aulas mais dinâmicas."

"Pouco aplicada na realidade, cotidiano do aluno."

"Alunos com pouca compreensão dos conteúdos matemáticos."

"A motivação é dependente do grupo de alunos em que se aplica a proposta"

"Assim como pode ser motivador para alguns, para outros pode não ser, vai do professor buscar estratégias diferenciadas de como abordar o conteúdo em sala."

"Os aluno não se motivam por quase nada em sua maioria."

"Acho que em alguns momentos é bem interessante e desafiador."

Nível 4:

"Pode fazer com os alunos tenham mais interesse na disciplina para perceber sua importância."

"É motivador porque torna a aula diferente da tradicional e pode motivar o aluno."

"Desperta o interesse pelo fato de poder escrever uma mensagem em código e ao mesmo tempo pode-se desvendar a matemática que há por trás da atividade."

"É pouco aplicada no cotidiano, talvez em uma aula dinâmica."

"É interessante trabalhar esse tema e desafiar os aluno."

"Acredito que vai motivar a maioria."

"Algo novo, e podem se comunicar de diferentes maneiras."

Nível 5:

"É desafiador."

"Tema curioso."

"É dinâmico e interativo."

"Você pretende utilizar toda ou parte desta oficina nas aulas do Ensino Fundamental?" foi a terceira pergunta feita aos participantes, dos quais 23 responderam que pretendem utilizar as atividades e apenas cinco não pretendem aproveitar.

A resposta afirmativa foi justificada pelos professores da seguinte forma:

"Interessante eles saberem como funciona alguns dispositivos."

"Auxilia no entendimento de conteúdos."

"Pretendo utilizar as tabelas para utilizar o algoritmo da divisão."

"Achei interessante, talvez signifique mostrar o conteúdo."

"Pretendo utilizar parte da oficina."

"A oficina mostrou-se interessante e atrativa, podendo ser aplicada em parte dependendo do nível da turma."

"Pois achei interessante."

"Parte a princípio. Iniciar e depois avaliar."

"Só algumas que podem ser aplicadas e também temos que ver qual delas. Depende da turma."

"Pois instiga a curiosidade."

"Depois que fazer uma análise da turma/classe, ou pequenos grupos."

"Por ver uma boa maneira de trabalha com a abstração dos códigos."

"Tem muito a ver com o conteúdo de álgebra, especialmente no 8º ano."

"Algumas atividade já são de certa forma abordadas, mas achei bem interessante algumas atividades que acredito serem de fácil entendimento pelos alunos."

"As mais simples podem ser utilizadas como um desafio."

"As atividades apenas."

"Pois para mim é bem aplicável."

"Alguns são bem acessíveis a eles e as quais ajudam a motivá-los."

"Porque algumas turmas tem muitas dificuldades e defasagens."

Já a resposta "não" , os docentes justificaram da seguinte forma:

"Somente a Cifra de Cesar pq. é de interesse do aluno."

"Algumas atividades são de boa aceitação."

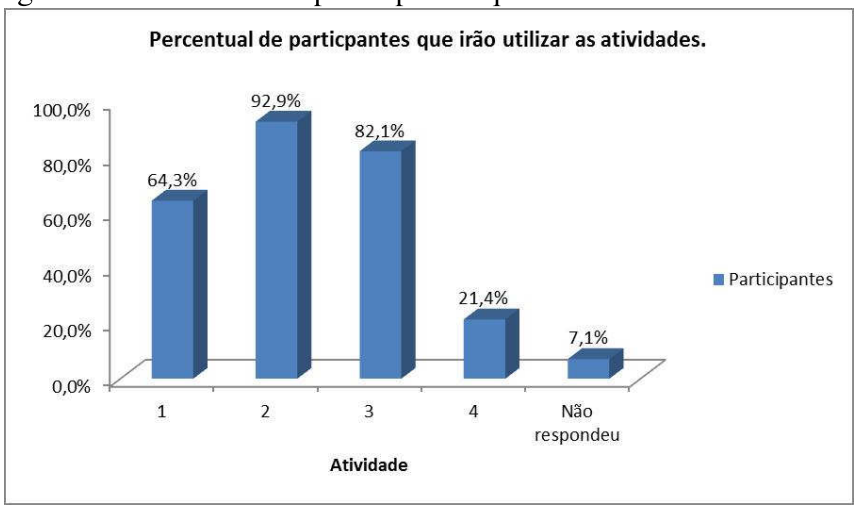
"Pois algumas são complexas para o nível dos nossos alunos."

"Há muita defasagem no conhecimento, que causaria mais "euforia"do que aprendizagem significativa."

As respostas para a pergunta 4 "Se utilizar, qual(quais) atividade(s)?" estão apresentadas no gráfico da Figura 10. Vale destacar que as pessoas que disseram que não irão utilizar as

atividades na questão anterior responderam a esta pergunta.

Figura 10: Percentual de participantes que irão utilizar as atividades.

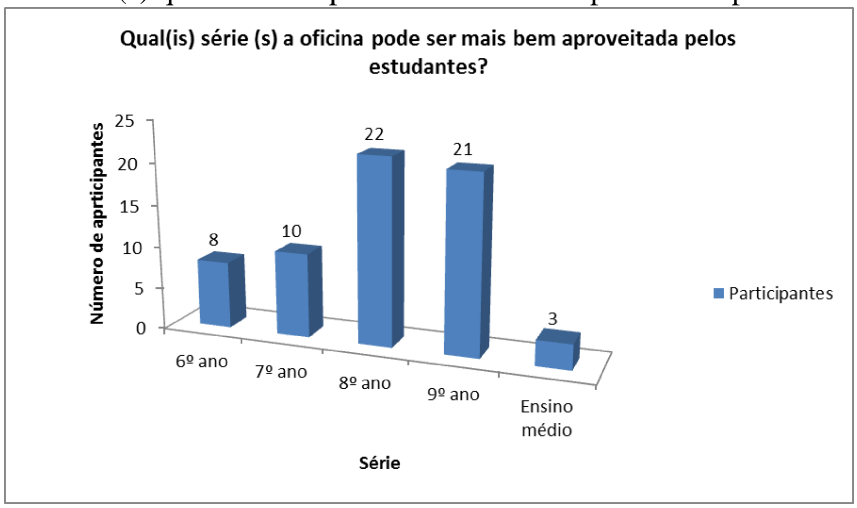


Fonte:Autor.

De um modo geral, as atividades (1), (2) e (3) tiveram melhor aceitação entre os participantes. A perspectiva da baixa utilização da atividade (4) se justifica devido ao uso do termo congruência. Isso também pode ser atribuído ao fato do tempo para a realização da oficina, o que impossibilitou a apresentação deste conceito de forma mais adequada aos docentes.

"Para qual série abaixo a oficina pode ser mais bem aproveitada pelos estudantes?" foi a quinta questão cujas respostas estão representadas no gráfico da Figura 11:

Figura 11: Série(s) que a oficina pode ser mais bem aproveitada pelos estudantes.



Fonte:Autor.

Nesta questão há um entendimento por parte do grupo de que as atividades propostas serão mais bem aproveitadas no 8º e 9º ano.

Na questão 6 foi solicitado para deixar sugestões e comentários obtendo as as seguintes respostas:

*"Acredito que * que foi trabalhado, foi bem explicativo, esclarecido."*

"Mais tempo para executar e sanear as possíveis dúvidas."

"Fiz alguns comentário na folha de atividades."

"Parabéns pelas atividades, adorei a oficina."

"Oficina bem produtiva, bem dinâmica."

"Pensar em uma linguagem mais simples para ser usada com os alunos. Para facilitar a comunicação."

"Algo novo para mim. Bom."

"Boas atividades e desafiadoras."

De um modo geral, a oficina teve boa aceitação para este grupo de docentes, como se confirma pela quantidade de professores que responderam que irão aproveitar as atividades com seus alunos. Contudo, algumas adaptações podem facilitar a aplicabilidade com os alunos, como por exemplo, um tempo maior para a explicação das práticas e a supressão do tema congruência, aprofundar e dispor de um tempo maior para se trabalhar com os alunos o conceito de algoritmo da divisão.

As atividades propostas revelaram-se de grande importância para o desenvolvimento docente. Por meio das atividades, eles conheceram sobre a Cripografia, que pode-se associar conceitos abstratos da Matemática com o cotidiano do aluno e verificaram a possibilidade de utilização em sala de aula. Os professores mostraram a intenção de utilizar o material didático com seus alunos, atendendo um dos objetivos deste trabalho e que o material desenvolvido pode motivar o aluno na aprendizagem da Aritmética.

5 CONSIDERAÇÕES FINAIS

A criptografia está presente na sociedade, conforme visto neste trabalho, desde antes de Cristo. Ela esteve em momentos importantes e decisivos na história, bem como envolve conceitos matemáticos no desenvolvimento de seus algoritmos. A aprendizagem da Matemática está cercada de complexidades em ambientes repletos de obstáculos, como a falta de motivação dos alunos, dificuldade na contextualização de conceitos matemáticos com o cotidiano, além das barreiras na construção do pensamento e do raciocínio lógico.

Neste trabalho foi apresentada uma proposta didática para minimizar os obstáculos que os alunos enfrentam na aprendizagem da Matemática, mais especificamente no ramo da Aritmética, através do uso da Criptografia.

Conheceu-se sobre a Criptografia, um pouco de sua história, seu funcionamento e usos, em especial a Criptografia RSA, o algoritmo de segurança mais utilizado na atualidade. Com essa pesquisa, buscou-se motivar o professor da Educação Básica na aprendizagem de conceitos como divisibilidade e números primos e com isso utilizar e trabalhar com seus alunos esse conhecimento adquirido. Confirmou-se que conteúdos matemáticos obrigatórios elencados na BNCC são base da Criptografia RSA, e consequentemente, passíveis de produzirem materiais didáticos relacionando a Matemática e a Criptografia, servindo como estímulo para a aprendizagem.

Para atingir o objetivo proposto, estabeleceu-se uma forma de abordagem que permitiu apresentar conceitos de Aritmética na Educação Básica relacionando-os com a Criptografia para estimular o aluno e auxiliá-lo na construção do conhecimento. Para tanto, foram elaborados materiais didáticos alternativos que se apropriaram de conceitos de Matemática e sua relação com a Criptografia.

As atividades foram aplicadas em forma de oficina para um grupo de docentes do Ensino Fundamental atuantes do sexto ao nono ano da rede pública municipal, que puderam averiguar e afirmar a aplicabilidade destas práticas.

Conforme relatado pelos docentes um dos desafios para implementação e utilização em sala de aula é a quantidade de alunos por turma e os diferentes níveis de compreensão dos alunos. Todavia, a oficina proposta foi aceita pelos docentes de forma satisfatória. Isso foi comprovado pelos depoimentos e pelo interesse em desenvolver as atividades propostas demons-

trados pelos professores. Ao mesmo tempo em que foram obtidos bons resultados, também se recebeu sugestões de adaptação para facilitar a aplicabilidade das atividades ofertadas. Além disso, obteve-se o relato de alguns docentes afirmando que utilizarão algumas atividades em sala de aula com seus alunos, confirmando o sucesso deste trabalho.

Constatou-se ainda, com o desenvolvimento deste trabalho, que a Criptografia pode ser introduzida nas aulas de Matemática na Educação Básica, com o objetivo de motivar os alunos, partindo de uma aplicação de conceitos de Aritmética e relacionando-os com a Criptografia.

Este trabalho contribuiu para aumentar a motivação dos alunos, colaborando com o conhecimento necessário, minimizando os desafios presentes na atividade docente. Além disso, forneceu embasamento teórico para que os alunoss construam suas próprias argumentações, podendo ser utilizado como estímulo para o desenvolvimento do gosto da Matemática por parte do aluno, aprimorando o seu raciocínio lógico, ensinando-o a pensar na Matemática por meio de situações reais, cativantes e motivadoras.

Como proposta de continuidade deste trabalho serão aplicadas as atividades (5), (6) e (7) para os professores participantes da oficina. Para pesquisas futuras sugere-se realizar as adaptações propostas nas atividades pelos docentes e aplicá-las em sala de aula com posterior análise das percepções dos alunos ao tema Criptografia como motivação para o estudo da Aritmética na Educação Básica.

REFERÊNCIAS

BARBOSA, G. **Números Primos e o Teorema Fundamental da Aritmética no Sexto Ano do Ensino Fundamental**. Dissertação (Mestrado) — IMPA, 2015.

BRASIL. **Base Curricular Nacional**. Brasília: MEC, 2017.

CALDWELL, C. K. **The Largest Known Primes–A Summary**. 2017. Disponível em: <http://primes.utm.edu/largest.html>. Acesso em: 14-02-2018.

CARVALHO, L. R. d. **O uso de elementos da criptografia como estímulo matemático na sala de aula**. Dissertação (Mestrado) — Universidade Estadual Paulista (UNESP), 2016.

COUTINHO, S. C. **Criptografia**. [S.l.]: Rio de Janeiro, IMPA/SBM, Programa de Iniciação Científica da OBMEP, 2007.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: IMPA, 2014.

Enciclopédia Culturama. **Biografia de Heródoto. Historiador Grego**. 2015. Disponível em: <https://edukavita.blogspot.com.br/2015/06/biografia-de-herodoto-historiador-grego.html>. Acesso em: 26-10-2017.

ENCRIPTADOS. 2015. Disponível em: <https://encriptados.wordpress.com/fotografias/>. Acesso em: 17-02-2018.

ENIGMA I The Service Enigma Machin. 2017. Disponível em: <http://www.cryptomuseum.com/crypto/enigma/i/index.htm>. Acesso em: 17-02-2018.

FIARRESGA, V. M. C. **Criptografia e matemática**. Dissertação (Mestrado) — Universidade de Lisboa, 2010.

GIL, K. H. et al. **Reflexões sobre as dificuldades dos alunos na aprendizagem de Álgebra**. Dissertação (Mestrado) — Pontifícia Universidade Católica do Rio Grande do Sul, 2008.

GIMENEZ, J.; LINS, R. **Perspectivas em aritmética e álgebra para o século XXI**. Campinas: Papirus Editora, 1997.

GROENWALD, C. L. O.; SAUER, L. de O.; FRANKE, R. F. A história da matemática como recurso didático para o ensino da teoria dos números e a aprendizagem da matemática no ensino básico. **Paradígma**, v. 26, n. 2, p. 35–55, 2005.

HEFEZ, A. **Aritmética**. [S.l.]: Rio de Janeiro: SBM, 2014.

HYGINO, H. D. **Fundamentos de Aritmética**. [S.l.]: Atual Editora-São Paulo, 1991.

JÚNIOR, E. M. da C.; VIEIRA, M. L.; CAETANOS, N. G. A criptografia em sala de aula. **Revista do Professor de Matemática (RPM)**, v. 89, p. 32–34, 2015.

LOUREIRO, F. O. **Tópicos de criptografia para o ensino médio**. Dissertação (Mestrado) — Universidade Estadual do Norte Fluminense, 2014.

MALTA, I. Linguagem, leitura e matemática. **Disciplinas Matemáticas em Cursos Superiores.**, EDIPUCRS, Rio de Janeiro, v. 1, 2004.

MILIES, F. C. P.; COELHO, S. P. **Números: uma introdução à matemática**. São Paulo: Edusp, 2001.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. **Revista Segurança Digital**, Brasília, v. 2, n. 3, p. 21–24, 2012.

PEREIRA, A. I.; PACHECO, M. F.; FERNANDES, F. P. Jogos matemáticos como ferramenta para motivar os estudantes para aprender matemática. In: IPB. **VII Congresso Mundial de Estilos de Aprendizagem**. [S.l.], 2016. p. 3029–3036.

SÁ, Ilydio Pereira de. **Aritmética Modular e Algumas de suas Aplicações**. Disponível em: <http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf>. Acesso em: 20-04-2018.

SANTOS, A. P. F. d. **A Criptografia no ensino mé fundamental II: contexto histórico, cifras simétricas, aplicação de conteúdos matemáticos e muitas outras curiosidades**. Dissertação (Mestrado) — Universidade no Norte Fluminense, 2016.

SCHLIEMANN, A. D.; CARRAHER, D. W.; CARRAHER, T. N. **Na vida dez, na escola zero**. São Paulo: Cortez, 1995.

SILVA, I. N. d. **Criptografia na educação básica: das escritas ocultas ao código RSA**. Dissertação (Mestrado) — PUC-Rio, 2016.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2001.

SINGH, S. **O livro dos códigos**. Rio de Janeiro: Record, 2007.

TAMAROZZI, A. C. Codificando e decifrando mensagens. **Revista do professor de matemática**, v. 45, p. 41–43, 2001.

TEIXEIRA, L. R. M. Dificuldades e erros na aprendizagem da matemática. **VII Epem Encontro Paulista de Educação Matemática**, 2004.

TERRADA, R. Criptografia e a importância das suas aplicações. **Revista do Professor de Matemática (RPM)**, v. 12, 1988.

VIANA, M. **A criptografia moderna não existiria sem os números primos.** Folha de S. Paulo, 2017. Disponível em: <http://www1.folha.uol.com.br/colunas/marceloviana/2017/09/1922755-a-criptografia-moderna-nao-existiria-sem-os-numeros-primos.shtml>. Acesso em: 09 de setembro de 2017.

APÊNDICE A – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

A Criptografia como motivação para o estudo da Aritmética na Educação Básica.

Prezado participante,

Você está sendo convidado(a) a participar da pesquisa **A Criptografia como motivação para o estudo da Aritmética na Educação Básica**.

Desenvolvida por Reginaldo Cristiano Griseli, discente de Mestrado Profissional de Matemática em Rede(PROFMAT) da Universidade Federal da Fronteira Sul (UFFS), Campus de Chapecó, sob orientação da Professora Dr. Janice Teresinha Reichert.

O objetivo central do estudo é: realizar uma oficina relacionando Criptografia com conteúdos da Aritmética ensinados no Ensino Básico.

O convite a sua participação se deve à importância de estabelecer uma forma de abordagem que permita apresentar conceitos de Aritmética na educação básica relacionados com a Criptografia que motive o estudante e que o auxilie na construção do pensamento e do raciocínio lógico.

Sua participação não é obrigatória e você tem plena autonomia para decidir se quer ou não participar, bem como desistir da colaboração neste estudo no momento em que desejar, sem necessidade de qualquer explicação e sem nenhuma forma de penalização. Você não será penalizado de nenhuma maneira caso decida não consentir sua participação, ou desista da mesma. Contudo, ela é muito importante para a execução da pesquisa.

Você não receberá remuneração e nenhum tipo de recompensa nesta pesquisa, sendo sua participação voluntária.

Serão garantidas a confidencialidade e a privacidade das informações por você prestadas. Qualquer dado que possa identificá-lo será omitido na divulgação dos resultados da pesquisa e o material armazenado em local seguro.

A qualquer momento, durante a pesquisa, ou posteriormente, você poderá solicitar do pesquisador informações sobre sua participação e/ou sobre a pesquisa, o que poderá ser feito através dos meios de contato explicitados neste Termo.

A sua participação consistirá em responder perguntas de um roteiro de questionário ao pesquisador da oficina. Você será convidado a participar de atividades que envolvam conteúdos matemáticos, preenchendo materiais pré-confecionados, realizando cálculos, respondendo questionamentos, participando e colaborando durante a oficina.

Poderão ser realizadas fotos e/ou filmagem da realização das atividades, porém sem a identificação dos participantes.
As atividades serão realizadas no local cedido pela Secretária Municipal de Educação de Chapecó.
O tempo de duração das atividades e do preenchimento dos questionários é de três turnos de aproximadamente duas horas e trinta minutos cada.
Os materiais preenchidos durante a oficina serão recolhidos para análise, transcritos e armazenadas, em arquivos digitais, mas somente terão acesso às mesmas o pesquisador e sua orientadora, podendo partes e/ou sua totalidade fazerem parte da dissertação.
Ao final da pesquisa, todo material será mantido em arquivo, físico ou digital, por um período de cinco anos.
O benefício relacionado com a sua colaboração nesta pesquisa é o de participar de uma oficina que tenha como finalidade propor materiais didáticos que possam ser usados em sala de aula para alunos de sexto ao nono ano do ensino fundamental.
A participação na pesquisa poderá causar riscos de constrangimento durante a oficina que serão minimizados e/ou totalmente eliminados através da condução da oficina. Os resultados serão divulgados em eventos e/ou publicações científicas mantendo sigilo dos dados pessoais.

Caso concorde em participar, uma via deste termo ficará em seu poder e a outra será entregue ao pesquisador. Não receberá cópia deste termo, mas apenas uma via. Desde já agradecemos sua participação!

Chapecó, _____de _____de 2018

Reginaldo Cristiano Griseli
Tel: (xx)xxxx-xxxx
e-mail: reginaldogriseli@hotmail.com
Endereço para correspondência: Universidade Federal da Fronteira SulUFFS, Rodovia SC 484 Km 02, Fronteira Sul, CEP 89815 899 Chapecó Santa Catarina Brasil

Declaro que entendi os objetivos e condições de minha participação na pesquisa e concordo em participar.

Nome completo do (a) participante: _____
Assinatura: _____

APÊNDICE B – QUESTIONÁRIO INICIAL

Nome:_____

Oficina: A Criptografia como motivação para o estudo da Aritmética na Educação Básica.

Questionário inicial:

1 - Marque qual série você atua no momento, no Ensino Fundamental, e há quanto tempo?

( ) 6º ano Tempo: _____
( ) 7º ano Tempo: _____
( ) 8º ano Tempo: _____
( ) 9º ano Tempo: _____
Outro:_____ Tempo: _____

2 - Descreva o que você trabalha com cada conteúdo abaixo:

•Números inteiros_____

•Números primos:_____

•Divisibilidade:_____

•Mínimo múltiplo comum (mmc):_____

•Máximo divisor comum (mdc):_____

3 - Quais dos conceitos abaixo você trabalha com seus alunos? Marque com um X o nível de dificuldade dos alunos de 1 a 5 para assimilar os conceitos, sendo 1 pouca dificuldade e 5 muita dificuldade?

	Trabalha		**Dificuldade**				
Conceito	**Sim**	**Não**	**1**	**2**	**3**	**4**	**5**
Números inteiros:							
Números primos:							
Divisibilidade:							
Mínimo múltiplo comum (mmc):							
Máximo divisor comum (mdc):							

4 - Qual é sua resposta quando o aluno pede por que estudar número primo?

_____

5 - Você tem conhecimento sobre criptografia? Sim_____ Não _____ Se sim cite um exemplo de onde ela é utilizada:

6 - Você considera que a criptografia tem relação com conceitos matemáticos?

Sim_____ Não _____

7 - Que conceitos matemáticos você considera que sejam utilizados para criptografar códigos?

8 - Você já tem conhecimento sobre criptografia de substituição, transposição e RSA?

Sim_____ Não _____

9 - Você considera o tema criptografia motivador para o ensino de Matemática aos alunos do Ensino Fundamental? Marque 1 para nada motivador e 5 muito motivador.

Motivação: 1 ( ) 2 ( ) 3 ( ) 4( ) 5 ( )

Justifique sua resposta:

APÊNDICE C – ATIVIDADE 1 = CÍTALA (TRANSPOSIÇÃO)

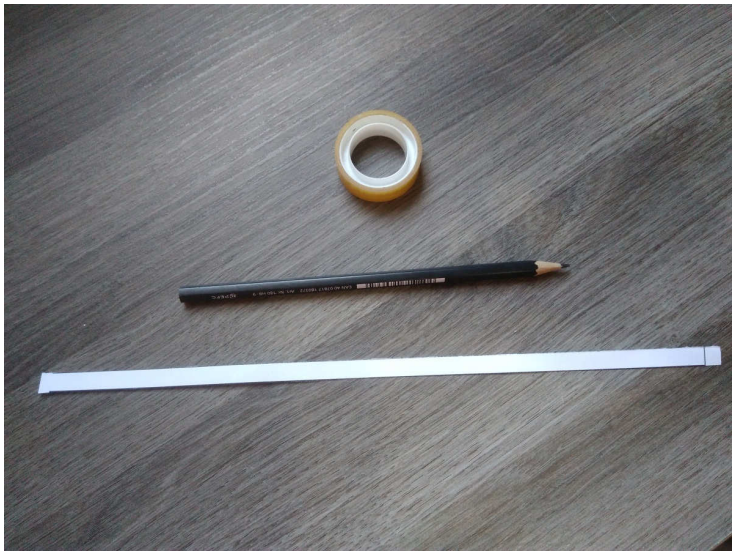
Nome:_____

Atividade 1 = Cítala (transposição)

A cítala ou bastão de Licurgo foi utilizada no século V a.C. pelos espartanos. Eles utilizavam um bastão de madeira, onde era enrolada uma tira de couro ou papiro, no qual era escrita uma mensagem ao longo do comprimento, sendo desenrolada e transportada como um cinto, com as letras voltadas para o corpo. O mensageiro entregava o código ao destinatário, o qual possuía um bastão idêntico ao do remetente, conhecendo a mensagem ao enrolar a fita (SINGH, 2007, pag. 24). Esse método usado na cítala é chamado de transposição onde as letras são misturadas formando anagramas.

Atividade 1.1: Construir cítala caseira.

Materiais: um lápis (de preferência sextavado); uma tira de 1 cm de largura feita do comprimento de uma folha A4; fita adesiva.



Modo: Enrole a tira no lápis e prenda as pontas com fita adesiva; escreva a mensagem no sentido horizontal do lápis; desenrole a tira do lápis e escreva a mensagem codificada na sequência da tira.

Atividade 1.2: Escreva uma mensagem criptografada usando a cítala caseira e passe para o colega.

Mensagem enviada:_____

_____

Mensagem criptografada:_____

._____

Atividade 1.3: Descreva nas linhas abaixo a mensagem recebida do colega, decodificando-a.
Mensagem criptografada recebida:_____

_____

Mensagem decodificada recebida:_____

_____

Atividade 1.4: Usando a tabela abaixo, escreva uma mensagem (escreva no sentido horizontal da tabela) e passe para o colega a mensagem criptografada. Para criptografar, transcreva as letras da tabela na ordem que aparecem nas colunas da tabela, inserindo um traço quando existir espaço entre as palavras.

Mensagem enviada:_____

_____

Mensagem criptografada:_____

_____

Atividade 1.5: Descreva nas linhas abaixo a mensagem recebida do colega usando a tabela abaixo.

Mensagem criptografada recebida:_____

_____

Mensagem decodificada: _____

_____

Questão 1: Você encontrou alguma dificuldade no desenvolvimento desta atividade? Qual?

_____

_____

_____

Questão 2: Você considera que essa atividade possa ser desenvolvida com os estudantes do Ensino Fundamental?

_____

_____

Questão 3: Se sim, em qual ano?

_____

APÊNDICE D – ATIVIDADE 2 = CIFRA DE CÉSAR(SUBSTITUIÇÃO)

Nome:_____

Atividade 2 = Cifra de César(substituição)

Este método, chamado de substituição, foi usado por Júlio César (Imperador Romano de 49 a.C a 44 a.C.), que consistia na troca cada letra da mensagem original por outra letra do alfabeto, seguindo um padrão. Essa Criptografia foi usada nas Guerras da Gália de Júlio César, ficando conhecida como Cifra de César.

Atividade 2.1: Criar um dispositivo para encriptação e decriptação de mensagens, baseado em copos descartáveis, para se trabalhar com sistemas criptógrafos baseados na cifra de César.

Materiais: Dois copos grandes de plástico descartável; Duas tiras de papel de comprimento igual ao da circunferência da boca do copo.

Modo: Escrever o alfabeto com as 26 letras nas tiras e fixá-las na borda do copo;

Decifre a mensagem Criptografada ”XLEPXLETNL”, tendo como chave a Letra L.
Mensagem: XLEPXLETNL

Mensagem decodificada:_____

Devido a frequência do uso das letras de um determinado idioma é possível uma pessoa decifrar essa forma de envio de mensagem. Segundo SINGH (2007, pág. 24), a fragilidade dessa forma de Criptografia causou a condenação à morte da rainha da Escócia Maria Stuart (1542 - 1587). Ela planejava matar sua prima, a rainha Elizabeth I da Inglaterra, enviando mensagens para seus aliados substituindo letras e algumas palavras recorrentes por símbolos. Mas as mensagens foram interceptadas e decifradas servindo como prova contra a rainha da Escócia.

Atividade 2.2: Redija uma mensagem, escolhendo uma chave, e repasse para que o colega a decifre.

Mensagem enviada:_____

Chave: _____

Mensagem criptografada:_____

Atividade 2.3: Descreva nas linhas abaixo a mensagem recebida do colega.

Chave: _____

Mensagem criptografada recebida:_____

_____

Mensagem decodificada recebida:_____

_____

Questão 1: Você encontrou alguma dificuldade no desenvolvimento desta atividade? Qual?

_____

_____

_____

Questão 2: Você considera que essa atividade possa ser desenvolvida com os estudantes do Ensino Fundamental?

_____

_____

Questão 3: Se sim, em qual ano?

_____

APÊNDICE E – ATIVIDADE 3 =APLICANDO MATEMÁTICA RELACIONADA À ATIVIDADE 2

Nome:_____

Atividade 3 =Aplicando Matemática relacionada à atividade 2

Note que ao numerarmos as letras do alfabeto podemos ter a seguinte tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

Tabela: 1

Atividade 3.1: Transforme a palavra Matemática em números utilizando a tabela 1 :

M	A	T	E	M	A	T	I	C	A

Atividade 3.2: Criptografe usando o algoritmo de Euclides utilizando a tabela abaixo tendo como chave L=11:

Letra original	**Letra em números (tabela 1)**	**Valor da letra somada a chave L=11**	**Algoritmo da divisão (divisor=26)**	**Codificação (resto da divisão)**	**Mensagem criptografada**
M	12				
A	0				
T	19				
E	4				
M	12				
A	0				
T	19				
I	8				
C	2				
A	0				

Atividade 3.3: Usando a Matemática, decodifique a mensagem anterior.

Mensagem criptografada	**Valor correspondente à tabela 1**	**Valor diminuído pela chave L=11**	**Resultado**	**Ajuste do valor negativo**	**Mensagem decodificada**	**Mensagem original**
X						
L						
E						
P						
X						
L						
E						
T						
N						
L						

Atividade 3.4: Codifique as palavras abaixo usando a chave contida na tabela.

Letra original	**Letra em números (tabela 1)**	**Valor da letra somada a chave G=6**	**Algoritmo da divisão (divisor=26)**	**Codificação (resto da divisão)**	**Mensagem criptografada**
C					
H					
A					
P					
E					
C					
O					

Palavra criptografada: _____

Letra original	**Letra em números (tabela 1)**	**Valor da letra somada a chave T=19**	**Algoritmo da divisão (divisor=26)**	**Codificação (resto da divisão)**	**Mensagem criptografada**
H					
A					
R					
M					
O					
N					
I					
A					

Palavra criptografada: _____

Atividade 3.5: Decodifique as palavras abaixo usando o algoritmo de divisão. Palavra criptografada:OPKPXMCZ Chave:11

Mensagem criptografada	**Valor correspondente à tabela 1**	**Valor diminuído pela chave** ----	**Resultado**	**Ajuste do valor negativo**	**Mensagem decodificada**	**Mensagem original**

Palavra decodifica: _____

Palavra criptografada:DOHJULD Chave:3

Mensagem criptografada	**Valor correspondente à tabela 1**	**Valor diminuído pela chave** ----	**Resultado**	**Ajuste do valor negativo**	**Mensagem decodificada**	**Mensagem original**

Palavra decodifica: _____

Atividade 3.6: Decodifique a frase abaixo usando o algoritmo de divisão e/ou usando os copos usados na atividade 2.(Utilize a chave E=4)

Frase codificada:EGVIHMXI, ZSGI TSHI XYHS

Frase decodificada:_____

Questão 1: Você encontrou alguma dificuldade no desenvolvimento desta atividade? Qual?

_____

_____

_____

Questão 2: Você considera que essa atividade possa ser desenvolvida com os estudantes do Ensino Fundamental?

_____

_____

Questão 3: Se sim, em qual ano?

_____

APÊNDICE F – ATIVIDADE 4 = CONGRUÊNCIA

Nome:_____

Atividade 4 = Congruência

Você notou que podemos usar o algoritmo da divisão para calcular as horas?

Ex.:Que horas serão as 17 horas, considerando as horas de 1 a 12?

$17 = 12 \cdot 1 + 5$ ou seja,
$D = d \cdot q + r$, onde:
17 é o dividendo;
1 é o quociente;
12 é o divisor e
o resto é 5.

Atividade 4.1: Utilizando o algoritmo da divisão calcule:
a) Que horas são 23 (considerando as horas de 1 a 12)?
Processo: $23 = 1 \cdot 12 + 11$, portanto são 11 horas.

Podemos demonstrar por $23 \equiv 11 \bmod 12$, ou seja, 23 é congruente a 11 módulo 12, (restos iguais).

Este método foi usado na cifra de César, pois tínhamos 26 letras no alfabeto ao invés das 12 horas, nosso divisor é 26, o dividendo é cada número da mensagem, o quociente deve ser o maior possível, e o resto é o valor da letra.

Curiosidade: O conceito de congruência foi introduzido por Karl Friedrich Gauss (1777-1855) em seu livro *Disquisitiones Arithmeticae* de 1801. As notações de congruência presentes no livro são utilizadas até hoje. Gauss escreve em seu livro que foi induzido a usar o símbolo $\equiv$ devido a enorme analogia com a igualdade algébrica.

Atividade 4.2: Efetue as divisões e descreva o resultado usando o algoritmo da divisão: $D = d \cdot q + r$ e também congruência: D $\equiv$ r mod m.

a) 44:5 Algoritmo: --------- Congruência: ---------	c)1253:125 Algoritmo: --------- Congruência: ---------
b)1285:100 Algoritmo: --------- Congruência: ---------	d) 44:4 Algoritmo: --------- Congruência: ---------

Atividade 4.3: Dada a tabela abaixo, responda:

0	7	14	21	28	35	42	49	56...
1	8	15	22	29	36	43	50	57...
2	9	16	23	30	37	44	51	58...
3	10	17	24	31	38	45	52	59...
4	11	18	25	32	39	46	53	60...
5	12	19	26	33	40	47	54	61...
6	13	20	27	34	41	48	55	62...

a) Qual dia da semana cairá daqui 60 dias.

b) Qual dia da semana será daqui 534 dias?

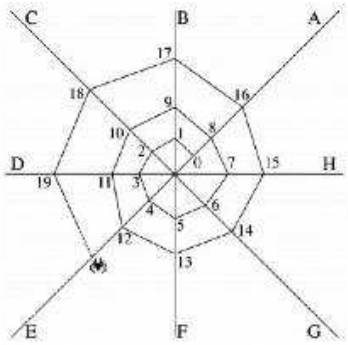
c) Como você poderia descrever todos os números que estão na mesma linha que o zero? E na linha do 1? E na linha do 4?

Atividade 4.4: Sabendo que o dia 19 de julho de 2018 é uma quinta-feira, determine, através

de cálculos, que dia da semana será o Natal de 2018.

Dica: Podemos utilizar a ideia das teias de aranhas para mostrar a congruência.

Figura:Teia de aranha.



Fonte:http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf.

Questão 1: Você encontrou alguma dificuldade no desenvolvimento desta atividade? Qual?

_____

_____

_____

Questão 2: Você considera que essa atividade possa ser desenvolvida com os estudantes do Ensino Fundamental?

_____

_____

Questão 3: Se sim, em qual ano?

_____

APÊNDICE G – ATIVIDADE 5 =CODIFICAR USANDO CRIPTOGRAFIA RSA.

Nome:_____

Atividade 5 =Codificar usando Criptografia RSA.

A Criptografia RSA foi inventada por Ronald Rivest, Adi Shamir e Leonard Adleman, em 1978, no Laboratório de Ciências da Informação do Massachusetts Institute of Technolgy(MIT). É um sistema criptográfico com chaves assimétricas, baseando-se na facilidade de encontrar números primos grandes e ao mesmo tempo na enorme dificuldade prática em fatorar o produto de dois desses números (HEFEZ, 2014, p. 319 - 320). Este método de criptografia utiliza-se de propriedades da Teoria dos números, entre ele uma das variantes do Teorema de Euler.

IMPORTÂNCIA DESTE METÓDO:
-Mais conhecido e mais usado atualmente;
-Difícil de ser quebrada;
-Utiliza alguns conceitos matemáticos desenvolvidos no Ensino Fundamental.

Quando você faz uma compra através da internet com cartão de crédito, você deve informar o número dele. O envio pode ser realizado usando a criptografia RSA.

Está criptografia se utiliza de conceitos matemáticos para codificar.

Atividade 5.1(Exemplo): Enviar o cartão de crédito número 10957318. Como a Criptografia RSA usa-se de teoremas não ensinados na educação básica, iremos utilizar uma "receita de bolo" com conceitos ensinados no Ensino Fundamental para realizar a codificação através da criptografia RSA.

Receita para criptografar:

1)Escolha dois números primos maiores que 2 e chame-os de primo p e primo q;
p:_____;q:_____

2)Calcule a chave de codificação n;
n=p*q; n:_____

3)Calcule o fi de Euler, que é obtido utilizando a fórmula φ (n)=(p-1).(q-1);
φ (_____)=(_____-1).(_____-1)=_____

4)Escolha o menor número (E) possível maior que 2 para que o mdc(E,φ(n))=1. Esta escolha se dará através de tentativa e erro, iniciando pelo número 3.

5) Quebre a mensagem em blocos para serem menores de n e que não iniciem com 0 (Escolha aleatória).

6) Eleve cada bloco ao expoente E.

7)Obtenha o resto r do resultado do passo 6 dividido por n.
$\{b^E \equiv r(mod\ n)\}$ ou $\{b^E = x \cdot n + r\}$.

8) Anote em sequência os blocos. Essa sequência é a mensagem criptografada.

Obs.: Chamamos de φ(n) o número de elementos que corresponda ao números de inteiros positivos entre 0 e (n-1) que são primos com n, isso define a função φ(fi) de Euler.

Temos que $\varphi(n) = n - 1$ apenas se m for um número primo, senão $\varphi(n) < n - 1$.

Ex.: $\varphi(4) = 2$, pois
mdc(4,1)=1 ;
mdc(4,2)=2;
mdc(4,3)=1.

$\varphi(5) = 4$, pois
mdc(4,1)=1 ;
mdc(5,2)=1;
mdc(5,3)=1;
mdc(5,4)=1

Atividade 5.2: Seguindo o roteiro abaixo criptografe o seguinte número: **51729623**

Utilize os seguintes dados **p=5 e q=11 e E=7**

1)Escolha dois números primos maiores que 2 e chame-os de primo p e primo q;
p:**5**;q:**11**

2)Calcule a chave de codificação n;
n=p*q; n:_____

3)Calcule o fi de Euler, que é obtido utilizando a fórmula φ (n)=(p-1).(q-1);
φ (_____)=(_____-1).(_____-1)=_____

4)Escolha o menor número (E) possível maior que 2 para que o mdc(E,φ(n))=1. Esta escolha se dará através de tentativa e erro, iniciando pelo número 3.
(Neste exercício o E já foi dado no enunciado) E=_____

---

5) Quebre a mensagem em blocos para serem menores de n e que não iniciem com 0 (Escolha aleatória).

---

6) Eleve cada bloco ao expoente E.

---

7)Obtenha o resto r do resultado do passo 6 dividido por n.
$\{b^E \equiv r(mod\ n)\}$ ou $\{b^E = x \cdot n + r\}$.

8) Anote em sequência os blocos. Essa sequência é a mensagem criptografada.

Atividade 5.3: Usando a criptografia RSA, codifique o seguinte número: **37945201** Utilize os seguintes dados **p=3 e q=11 e E=7**

Questão 1: Você encontrou alguma dificuldade no desenvolvimento desta atividade? Qual?

Questão 2: Você considera que essa atividade possa ser desenvolvida com os estudantes do Ensino Fundamental?

Questão 3: Se sim, em qual ano?

APÊNDICE H – ATIVIDADE 6 = DECODIFICAR USANDO CRIPTOGRAFIA RSA.

Nome:_____

Atividade 6 = Decodificar usando Criptografia RSA

Receita para decodificar: Agora iremos decodificar a Criptografia RSA utilizando conceitos ensinados no Ensino Fundamental através do roteiro abaixo.

Atividade 6.1(Exemplo): Decodificar os blocos codificados do cartão de crédito obtidos na atividade 5.1 **(5-4-10-7-33-1-8)** utilizando Criptografia RSA. Lembre que o valor E=5, p=5 e q=7

1) Escreva os blocos para decodificação.

_____

2)Obtenha valor D que multiplicado pelo valor E tenha resto 1 quando dividido por φ (n), ou seja, $\{E \cdot D \equiv 1(mod\ \varphi(n))\}$ ou $\{E \cdot D = b \cdot (\varphi(n)) + 1\}$

. _____

_____

3)Eleve cada bloco codificado ao expoente D.

_____

_____

_____

_____

_____

_____

_____

_____

4)Obtenha o resto do resultado do passo 3 dividido por n. $\{a^D \equiv r(mod\ n)\}$ ou $\{a^D = x \cdot n + r\}$.

_____

5) Anote em sequência os blocos, e reúna em sequência novamente. Essa sequência é a mensagem decodificada.

Saiba: Apenas o site de compra ou o banco conhece os valores de **p**, **q** e **D**. Já os valores de **n** e **E** é de conhecimento público.

O segredo da Criptografia RSA é que temos uma operação **fácil de fazer**, n=p*q, porém **extremamente difícil de fatorar n sem conhecer p e q.**

A**tividade 6.2:** Seguindo o roteiro abaixo decodifique os seguinte blocos: 25-1-28-18-4-41-18-42. Utilize os seguintes dados p=5 e q=11 e E=7.

1) Escreva os blocos para decodificação.

2)Obtenha valor D que multiplicado pelo valor E tenha resto 1 quando dividido por φ (n), ou seja, $\{E \cdot D \equiv 1(mod\ \varphi(n))\}$ ou $\{E \cdot D = b \cdot (\varphi(n)) + 1\}$

.

3)Eleve cada bloco codificado ao expoente D.

4)Obtenha o resto do resultado do passo 3 dividido por n. $\{a^D \equiv r(mod\ n)\}$ ou $\{a^D = x \cdot n + r\}$.

5) Anote em sequência os blocos, e reúna em sequência novamente. Essa sequência é a mensagem decodificada.

Atividade 6.3: Usando a criptografia RSA, decodifique os seguintes blocos: 9-28-15-16-14-26. Use os seguintes dados p=3 e q=11 e E=7.

Questão 1: Você encontrou alguma dificuldade no desenvolvimento desta atividade? Qual?

Questão 2: Você considera que essa atividade possa ser desenvolvida com os estudantes do Ensino Fundamental?

Questão 3: Se sim, em qual ano?

APÊNDICE I – ATIVIDADE 7 = CRIPTOGRAFIA RSA (MENSAGEM)

Nome:_____

Atividade 7 = Criptografia RSA (Mensagem)

Para criptografar letras, vamos usar a tabela abaixo:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	
10	11	12	13	14	15	16	17	18	19	20	21	22	

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Espaço
23	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**99**

Tabela: 2

Atividade 7.1: Você recebeu a mensagem abaixo, decodifique sabendo que **p=3**, **q=11** e **E=7** usando o roteiro abaixo.

Os blocos criptografados são

18-15-15-6-23-4-20-3-23-18-15-15-1-16-29-2-17-10-15-15-12-8-20-25-10-23-7-18

1) Escreva os blocos para decodificação.

_____

2)Obtenha valor D que multiplicado pelo valor E tenha resto 1 quando dividido por φ (n), ou seja, $\{E \cdot D \equiv 1(mod\ \varphi(n))\}$ ou $\{E \cdot D = b \cdot q + 1\}$.

_____

_____

3)Eleve cada bloco codificado ao expoente D.

18:_____

15:_____

15:
6:
23:
4:
20:
3:
23:
18:
15:
15:
1:
16:
29:
2:
17:
10:
15:
15:
12:
8:
20:
25:
10:
23:
7:
18:

4)Obtenha o resto do resultado do passo 3 dividido por n.
$\{a^D \equiv r(mod\ n)\}$ ou $\{a^D = x \cdot n + r\}$.

5) Anote em sequência os blocos, e reúna em sequência novamente. Essa sequência é a mensagem decodificada.

6) Substitua a mensagem decodificada pelas letras da tabela 2.

Atividade 7.2: Codifique a mensagem da atividade 7.1 usando o método da criptografia RSA. Utilize p=3, q=11 e E=7.

Atividade 7.3: Você recebeu a seguinte mensagem criptografada abaixo, descubra a mensagem codificada usando o método da criptografia RSA, sabendo que p=5, q=7 e E=5

Os blocos critografados são
33-16-9-32-26-21-9-22-19-28

Atividade 7.4: Codifique a mensagem da atividade 7.3 usando o método da criptografia RSA sabendo que **p=5, q=7 e E=5**.

Questão 1: Você encontrou alguma dificuldade no desenvolvimento desta atividade? Qual?

_____

_____

_____

Questão 2: Você considera que essa atividade possa ser desenvolvida com os estudantes do Ensino Fundamental?

_____

_____

Questão 3: Se sim, em qual ano?

_____

APÊNDICE J – QUESTIONÁRIO FINAL

Nome:_____

Oficina: A Criptografia como motivação para o estudo da Aritmética na Educação Básica.

Questionário final:

1 - Você acha que a oficina pode ser aplicada no Ensino Fundamental do 6º ao 9º ano?
Sim_____Não_____ Por quê:_____
_____

2 - Você considera o tema criptografia motivador para os alunos do Ensino Fundamental? Marque 1 nada motivador e 5 muito motivador.
Motivação: 1 ( ) 2 ( ) 3 ( ) 4( ) 5 ( )
Justifique sua resposta:
_____
_____

3 - Você pretende utilizar toda ou parte desta oficina nas aulas do Ensino Fundamental?
Sim_____ Não_____Por quê:_____
_____
_____

4 - Se utilizar, qual(quais) atividade(s)?
( ) Atividade 1 = Cítala (transposição).
( ) Atividade 2 = Cifra de César(substituição).
( ) Atividade 3 = Aplicando Matemática relacionada à atividade 2.
( ) Atividade 4 = Congruência.
( ) Atividade 5 = Codificar usando Criptografia RSA.
( ) Atividade 6 = Decodificar usando Criptografia RSA.
( ) Atividade 7 = Criptografia RSA(Mensagem).

5 - Para qual série abaixo a oficina pode ser mais bem aproveitada pelos estudantes?

( ) 6º ano ( ) 8ª ano

( ) 7º ano ( ) 9º ano

Outra: _____

6 - Deixe sugestões e comentários?

_____

_____

_____