UNIVERSIDADE FEDERAL DE JATAÍ (UFJ)
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS EXATAS E TECNOLÓGICAS (CIEXA)
PROFMAT - MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

RAFAEL BENTO DA SILVA

Números Primos. A criptografia via RSA

Jataí, GO
2021

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS EXATAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES

E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo das Teses e Dissertações disponibilizado na BDTD/UFG é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFJ

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Jataí (UFJ) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFJ), regulamentada pela Resolução CEPEC no 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data. O conteúdo das Teses e Dissertações disponibilizado na BDTD/UFJ é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do material bibliográfico
[x] Dissertação [ ] Tese

2. Nome completo do autor:

RAFAEL BENTO DA SILVA

3. Título do trabalho:

NÚMEROS PRIMOS. A CRIPTOGRAFIA VIA RSA

4. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)
Concorda com a liberação total do documento [x] SIM [ ] NÃO1
[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:
a) consulta ao(à) autor(a) e ao(à) orientador(a);
b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.
O documento não será disponibilizado durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;

- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:
a) consulta ao(à) autor(a) e ao(à) orientador(a);
b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.
O documento não será disponibilizado durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Obs. Este termo deverá ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Luciana Aparecida Elias**, **Professor do Magistério Superior**, em 19/01/2022, às 16:09, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **RAFAEL BENTO DA SILVA**, **Discente**, em 19/01/2022, às 17:38, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2635679** e o código CRC **BE8D1EA6**.

Referência: Processo nº 23070.051498/2021-83 SEI nº 2635679

RAFAEL BENTO DA SILVA

Números Primos. A criptografia via RSA

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Unidade Acadêmica Especial de Ciências Exatas e Tecnológicas, da Universidade Federal de Jataí (UFJ), como requisito para obtenção do título de Mestre em Matemática.
Área de concentração: Matemática do Ensino Básico.

Orientadora Profa. Dra. Luciana Aparecida Elias

Jataí, GO
2021

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

SILVA, RAFAEL BENTO DA
Números Primos. A criptografia via RSA / RAFAEL BENTO DA SILVA. - 2021.
39 f.

Orientadora: Profa. Dra. LUCIANA APARECIDA ELIAS.
Dissertação (Mestrado) - Universidade Federal de Jataí, Unidade Acadêmica Especial de Ciências Exatas e Tecnológicas, Jataí, PROFMAT- Programa de Pós-graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RJ), Jataí, 2021.

1. Comunicação. 2. Criptografia. 3. RSA. 4. Código. I. ELIAS, LUCIANA APARECIDA, orient. II. Título.

CDU 51

UNIVERSIDADE FEDERAL DE GOIÁS

COORDENAÇÃO DE PÓS-GRADUAÇÃO - REGIONAL JATAÍ

ATA DE DEFESA DE DISSERTAÇÃO

Ata nº **26** da sessão de Defesa de Dissertação de RAFAEL BENTO DA SILVA, que confere o título de Mestre em **Matemática**, na área de concentração em **Matemática do Ensino Básico**.

No dia trinta de setembro de 2021, a partir das **15h30 horas**, realizou-se a sessão pública de Defesa de Dissertação integralmente por meio de tecnologias de comunicação à distância, intitulada **"**NÚMEROS PRIMOS. A CRIPTOGRAFIA VIA RSA**"** nas dependências da Universidade Federal de Jataí, cujos programas de pós-graduação stricto sensu, ora em funcionamento, estão provisoriamente vinculados à Universidade Federal de Goiás, em virtude de procedimentos técnicos relacionados à CAPES e a transferência da Biblioteca Digital de Dissertações e Tese (BDTD), justificando assim o aparecimento do nome das duas instituições nesse documento, uma no corpo do texto (UFJ), outra no cabeçalho (UFG). Os trabalhos foram instalados pela Orientadora, Professora Doutora Luciana Aparecida Elias (UAE de Ciências Exatas / UFJ) com a participação dos demais membros da Banca Examinadora: Professora Doutora Luciana de Oliveira Berretta (INF/UFG), membro titular externo; Professor Doutor Esdras Teixeira Costa (UAE de Ciências Exatas / UFJ), membro titular interno. Durante a arguição os membros da banca **( ) fizeram (X) não fizeram** sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Dissertação, sendo o candidato **aprovado** pelos seus membros. Proclamados os resultados pela Professora Doutora Luciana Aparecida Elias, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, no trinta dez de setembro de 2021.

TÍTULO SUGERIDO PELA BANCA

Documento assinado eletronicamente por **Luciana Aparecida Elias**, **Professor do Magistério Superior**, em 30/09/2021, às 16:25, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Luciana De Oliveira Berretta**, **Professora do Magistério Superior**, em 30/09/2021, às 16:25, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Esdras Teixeira Costa**, **Professor do Magistério Superior**, em 30/09/2021, às 16:25, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?

FOLHA DE MENÇÃO

Os Programas de Pós-Graduação stricto sensu, ora em funcionamento na Universidade Federal de Jataí (UFJ), em virtude de procedimentos técnicos relacionados à CAPES, continuam provisoriamente vinculados à Universidade Federal de Goiás (UFG), no entanto, todos os elementos pré-textuais do trabalho apresentado estão identificados como Universidade Federal de Jataí, em função da migração da BDTD ter ocorrido a partir de 16 de agosto de 2021, e pelo fato das pesquisas e produções estarem sendo realizadas na UFJ.

Resumo

A necessidade de comunicação via internet e a segurança de dados provocou um sério avanço dos computadores e tecnologias de informação. A cada dia via-se a necessidade de privacidade e segurança dessas informações nesses percursos, quando fazemos transações bancárias e quando mandamos mensagens por aplicativos de celular somos informados, mesmo não sabendo ao certo os processos, de que essas informações não serão divulgadas para além do necessário, ou seja, não sabemos qual o nível de proteção dessas informações e como nossa privacidade é preservada. Para que essas mensagens se tornem ilegíveis para quem não é seu devido destinatário, usa-se o que chamamos de criptografia, que é a arte de tomar um texto e transformá-lo num código que só deveria ser desfeito por quem realmente for do interesse do emissor da mensagem. Sabemos que todo o método de criptografia é passível de ser quebrado, mesmo que a intenção de seus criadores seja que isso nunca ocorra indevidamente, empenhando-se a fazer de forma que seja impossível, ou quase impossível de ser decodificado. Nesse trabalho vamos comentar sobre alguns tipos de criptografia bem como alguns caminhos para quebra de código, oferecendo um breve histórico dos métodos mais seguros e como eles chegaram lá, dando destaque a criptografia RSA, por utilizar em sua dinâmica números primos que é conteúdo do Ensino Básico e por ser o mais usado e considerado o mais seguro atualmente, com a consciência de que mais cedo ou mais tarde ele também será quebrado, e um mais avançado será desenvolvido. De modo geral, todos os métodos são baseados em operações matemáticas que podem ser abordadas em sala de aula, como divisão euclidiana, fatoração, números primos, funções e etc. são alguns dos conteúdos que podem ser explorados por meio da criptografia. Dessa forma esse trabalho visa dar um suporte ao leitor ou leitora que desejam solidificar os conceitos sobre comunicação, criptografia e números primos para que possam construir modelos e planos de aula de atividades em sala.

Palavras-Chave: Comunicação, Criptografia, RSA, código

Abstract

The necessity of communication via internet and the security of data provoked a serious advance of computers and technologies of information. Each day there was the necessity of privacy and security of these information in these pathways, when we make bank transactions and when we send messages through smartphone applications we are informed, even not knowing the processes, that these information will not be disclosed beyond the necessary, that is, we do not know the level of protection of these information and how our privacy is preserved. For these messages to become illegible for those who are not the recipient, what we call encryption is used, which is the art of taking a text and transforming it into a code that will only be cracked for whom the issuer of the message interests. We know that the entire method of encryption is liable to be broken, even if the intention of its creators is that this never happens unduly, committing themselves to make it in such a way that is impossible, or barely possible of being decoded. In this paper we will comment about some types of encryption, as well as some paths to decoding the code, offering a brief history of the most safe methods and how they reached it, highlighting the encryption RSA, for utilizing in its dynamics prime numbers, which is content of basic education, and for being the most used and considered the most safe lately, with the conscience that sooner or later it will also be decoded, and a more advanced one will be developed. In general, all methods are based in mathematical operations that can be approached in a classroom, like Euclidian division, factorization, prime numbers, functions an etc. are some of the contents that can be explored through encryption. Therefore, this paper intends to give the reader support that wish to solidify the concepts on communication, encryption and prime numbers so they can build models and lesson plans of activities in class.

Keywords: Comunication, Cryptography, RSA, code

Lista de tabelas

Lista de abreviaturas e siglas

PCNs	Parâmetros Curriculares Nacionais
MIT	Massachussets Institute of Technology
BNCC	Base Nacional Comum Curricular
GIMPS	Great Internet Mersenne Prime Search

Lista de ilustrações

Sumário

Introdução

No ano de 490 a. C. a Pérsia estava em guerras expansionistas enfrentando e vencendo quase todo o Oriente Médio, e um dos inimigos enfrentados era a Grécia. Em um determinado dia a Pérsia montou seu acampamento na planície de Maratona para atacar Atenas com seu exército, mas a Pérsia perdeu, não contava com uma emboscada dos atenienses, que chegaram de surpresa à planície.

Mas não é a esse fato que quero destacar nesse trabalho, mas a uma lenda que muitos acreditam sobre algo que aconteceu depois da vitória da Grécia sobre a Pérsia. Diz a lenda que Fidípedes, um dos melhores corredores das tropas atenienses, consciente da grandeza da vitória que seu exército acabara de conquistar, correu para dar a boa notícia em Atenas, mesmo ferido, o soldado correu 40 quilômetros que separa Atenas da planície de Maratona o mais rápido que pôde e quando chegou, disse: "Vencemos"e caiu morto em seguida.

A história foi contada por muito e muitos anos, até chegar aos ouvidos do Barão Pierre de Coubertin, organizador dos primeiros jogos olímpicos da era moderna, em Atenas, 1896. Ele incluiu a modalidade Maratona (corrida) nos jogos como símbolo supremo do espírito olímpico. Antes as corridas eram feitas ao redor dos estádios, com no máximo 8 quilômetros, como homenagem a Fidípedes, a corrida maratona teria $40,195$ quilômetros de distância.

Tudo isso para enviar uma mensagem de vitória. A necessidade de comunicação é inerente ao ser humano e sempre foi extremamente valorizada. E assim como toda a ciência, a comunicação também evolui, em alguns anos passamos das cartas aos e-mails, conseguimos nos comunicar com qualquer pessoa em qualquer lugar do planeta por áudio ou vídeo através da internet.

Essa evolução se mostrou extremamente necessárias nos últimos dois anos (2020-2021), onde muitos ficaram confinados em casa devido a pandemia do COVID-19, aulas foram transmitidas das casas dos próprios professores a turmas das mais variadas idades e tamanhos, e os alunos tiveram que assistir essas aulas de forma remota em suas próprias casas através dos seus celulares e computadores, o trabalho *home office* recebeu destaque devido a necessidade de ficarmos em casa. Muitas empresas adotaram essa técnica de trabalho mesmo depois de algumas liberações, percebendo a economia que isso gerava.

Mas essa facilidade na troca de informações também trouxe alguns problemas a humanidade, muitas dessas informações não são públicas, o sigilo e a privacidade ficaram ameaçados com toda essa facilidade, trazendo um novo desafio, a necessidade de se esconder essas mensagens. A criptografia é a ciência que estuda as formas de "esconder"mensagens,

de modo que não seja acessível a qualquer um, mas apenas àqueles a quem a mensagem é destinada.

Temos como público alvo o leitor ou leitora interessados em criptografia, comunicação, tecnologias e/ou matemática.

Temos como objetivo oferecer um material aos interessados e interessadas acima descritos um texto para aprofundamento desses conceitos, como um componete teórico, e um futuro aparato para a formulação de planos de aula de conteúdos como números primos, num contexto diferente do usual. Usando a história e evolução da criptografia até chegarmos na criptografia RSA e suas aplicações, a criptografia não é uma ciência estática, mas sempre se renova e evolui, concordamos com Singh (2004, p.11) quando ele afirma:

> "E evolução é um termo bem adequado, porque o desenvolvimento de códigos pode ser visto como uma luta evolutiva, já que qualquer código está sempre sob ataque dos decifradores. " (SINGH, 2004)

Dessa forma observamos, que houve todo um processo para a criptografia dos dias atuais chegar onde está. A cada novo método criado para criptografar uma mensagem, alguém surgia com a quebra do código e estabelecia uma regra para a decodificação daquele método. Hoje não é diferente, na era em que a informação se tornou uma mercadoria, muitos ainda procuram formas de quebrar os códigos atuais, e outros muitos buscam uma forma mais segura de enviar e receber mensagens e dados.

Os métodos atuais utilizam de artifícios matemáticos para criptografar mensagens, um dos temas mais usados são os números naturais e suas propriedades, assunto estudado em Teoria dos Números na graduação, e em Aritmética no Profmat, com um destaque nos números primos. Os números primos são considerados os elementos básicos de todos os números naturais, nesse trabalho trouxemos alguns dos resultados mais importantes envolvento esses números e qual a importância deles na criptografia.

E se esse assunto é tão atual e tão cotidiano, por que não abordá-lo em sala de aula? Um dos objetivos gerais dos PCNs (Parâmetros Curriculares Nacionais) é: "saber utilizar diferentes fontes de informação e recursos tecnológicos para adquirir e construir conhecimento." NACIONAIS (1998). Para que possamos utilizar as diferentes formas de informação, precisamos ter acesso a essa informação, mas muitas das informações encontram-se criptografadas, logo é necessária essa abordagem, mesmo que em pequena escala.

1 COMUNICAÇÃO

A comunicação sempre foi algo importante para o ser humano, a necessidade de entender o outro e de ser entendido acompanha a humanindade desde sempre, por isso vamos falar um pouco sobre esse processo nesse capítulo.

1.1 Definições

A palavra comunicação tem sua origem no latim *communicare* que significa algo como compartilhar, participar, tornar comum. Partindo disso podemos perceber que a comunicação vai além de passar informações, ela pressupõe interatividade entre quem fala e quem ouve.

O processo de comunicação possui alguns elementos básicos, vamos destacar alguns deles.

Definição 1.1.1 (Emissor)**.** É aquele que transmite a mensagem, o que inicia o processo comunicativo.

Definição 1.1.2 (Código)**.** É o conjunto de sinais escolhidos pelo emissor para estabelecer a comunicação, podendo ser verbal ou não verbal. Esse código pode ser por sinais, gestos, sons, textos, desenhos, entre outros.

Definição 1.1.3 (Mensagem)**.** É o objeto da comunicação, o assunto a ser tratado entre aquele que a envia e a recebe.

Definição 1.1.4 (Canal)**.** É o meio pelo qual a mensagem será passada, seja uma pessoa, um vídeo, um aúdio, e-mail, carta, ente outros.

Definição 1.1.5 (Receptor)**.** É aquele que recebe a mensagem transmitida pelo emissor.

Além de entender cada uma das definições acima dadas, é importante e necessário entender que o canal de comunicação, que é a ligação entre emissor e receptor, deve estar livre de ruídos ou quaisquer coisas que possam modificar ou impedir a mensagem de chegar de forma clara e objetiva ao receptor.

Desde a antiguidade a ideia de se expressar foi algo inerente ao ser humano, hoje podemos visitar o sítios arqueológicos, onde há mensagens pintadas nas cavernas contando o dia-a-dia daqueles que viviam naquela época. Até nos dias atuais percebemos a necessidade de entendermos o outro e de sermos entendidos, dentro desse processo de comunicação, desejamos que a mensagem certa seja passada. Concordamos com Laruccia (2004, p.93)

> "A comunicação é inevitável, porque, mesmo quando não queremos, estamos o tempo todo emitindo mensagens para o outro, não sendo possível voltar atrás naquilo que já foi comunicado, da mesma forma que a comunicação é irrepetível, pois todos estão continuamente mudando. Mesmo quando lemos um livro, ou assistimos a um mesmo filme pela segunda vez, esse filme não será para nós o mesmo filme."(LARUCCIA, 2004)

Percebemos então que a comunicação é algo que faz parte do ser humano e da sociedade que o cerca, por meio da comunicação uns com os outros informações são compartilhadas e conhecimentos são adquiridos, o desenvolvimento humano está intimamente ligado à comunicação.

1.2 Linguagens, códigos e suas tecnologias

A necessidade de se comunicar fez com que o homem criasse sons e símbolos que representassem a mensagem que ele queria passar, dessa forma surgiu a língua falada e escrita, além de vários outros canais diferentes para que sua menssagem seja entendida, nos PCNs Parte (2000, p.64) podemos encontrar:

> "A fala, a escrita, os movimentos corporais, arte estão intimamente ligados à cognição, à percepção, à ação, sendo expressões da cultura. Todos os sistemas procuram tornar os significados comunicáveis. As linguagens se afastam no plano da expressão, constituindo formas póprias de manifestação, e voltam a se encontrar no plano do conteúdo, pano de fundo da construção humana dos símbolos."(PARTE, 2000)

Concordamos também com Parte (2000, p.5), onde chama de linguagem a capacidade humana de organizar os mais variados significados coletivos de forma específica, levando em consideração as particularidades de cada indivíduo, comunidade, cultura e história.

Dessa forma percebemos que cada um tem uma linguagem diferente de passar a mesma mensagem, além de a linguagem ser diferente, podemos destacar também os canais diferentes de comunicação como o rádio, a televisão, o telefona, a internet, jornais, revistas, cinemas, entre outros.

Ao longo da história os meios de comunicação foram evoluindo junto com a humanidade, onde antes as cartas predominavam, veio o telégrafo, o telefone e o rádio logo em seguida, chegando hoje nas mensagens eletrônicas.

1.3 Uma linguagem secreta

O ser humano também sempre mostrou interesse na privacidade de informações pessoais, nesse trabalho vamos falar sobre criptografia, que é um tipo de comunicação

onde a mensagem passa por processos para que seja legível para o receptor, mas ilegível para todos os outros, ou seja, uma linguagem secreta.

A criptografia não está presente no currículo escolar, mas podemos perceber que várias das ideias usadas para os processos criptográficos são de conteúdos de matemática básica. Podemos citar por exemplo a ideia de função, principalmente a de função inversível, divisão de números inteiros e fatoração. Mas não apenas a parte dos conteúdos matemáticos, uma das competências trazidas para o Ensino Fundamental pela BNCC é:

> "Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados. " (EDUCAÇÃO, 2017)

Podemos entender a criptografia como uma ferramenta tecnológica de transmissão e acesso a informações. Então mesmo não focando no conteúdo trabalhado, a criptografia é uma linguagem matemática que pode ser analisada e trabalhada, gerando um pensamento algébrico, e uma facilidade no processo de criação e entendimento de algoritmos (pensamento computacional) para os alunos das séries finais do Ensino Fundamental. Mas não apenas para o Ensino Fundamental, os PCNs do Ensino Médio trazem também algumas competências que podemos destacar:

> "- . Desenvolver a capacidade de utilizar a Matemática na interpretação e intervenção no real.
> - Aplicar conhecimentos e métodos matemáticos em situações reais, em especial em outras áreas do conhecimento.
> - Relacionar etapas da história da Matemática com a evolução da humanidade.
> - Utilizar adequadamente calculadoras e computador, reconhecendo suas limitações e potencialidades." (TECNOLÓGICA, 1999)[p.46]

Assim podemos mais uma vez perceber que a criptografia pode ser considerada um assunto a ser abordado em sala de aula, tanto nas séries finais do Ensino Fundamental, quanto no Ensino Médio.

2 NÚMEROS PRIMOS

Conhecer os números primos pode parecer algo não muito útil, mas eles escondem uma beleza e importância que muitas vezes deixamos passar, sua utilidade está muito além de uma simples fatoração. Mas para entender sua aplicação, precisamos antes entender sua definição, história e alguns resultados importantes.

2.1 Definição

A ideia de números primos é apresentada na escola desde muito cedo, no sexto ano do Ensino Fundamental esse tema é abordado de forma precisa, principalmente no que se refere a operação de divisão, conceituação de divisores e de como achá-los e aplicá-los. Mas esse conceito é por muitas vezes esquecido com o passar do tempo, pois não é mais abordado em outros anos escolares, por vezes é mencionado quando necessário para um conteúdo subsequente, mas dificilmente aprofundado.

Assim que começamos a falar dos números naturais e suas propriedades, é comum no momento em que falamos da operação de divisão abordarmos os números primos, afinal sua definição tem tudo a ver com essa operação. Então vamos definir o que é um número primo:

Definição 2.1.1 (Números Primos)**.** Dizemos que um número é primo quando este possuir exatamente dois divisores naturais distintos, que são, o 1 e ele mesmo.

A partir dessa definição podemos listar os primeiros números primo, são eles: $2, 3, 5, 7, 11, 13, ...$, observamos que esses números têm exatamente dois divisores naturais distintos, o que não ocorre, por exemplo, com o número 6 que pode ser dividido por 2 e 3 além do 1 e o próprio 6. Dessa forma podemos acrescentar uma outra definição

Definição 2.1.2 (Números Compostos)**.** Dizemos que um número é composto quando possui mais de dois divisores naturais distintos

A partir dessas duas definições podemos perceber que o número 1 não se encaixa em nenhuma delas, pois esse número possui um único divisor, o próprio 1, sendo assim, não consideramos ele nem primo e nem composto.

Mas por que devemos estudar os números primos? Qual a importância deles? "Da mesma forma que os átomos são a estrutura básica da matéria, os números primos constituem a parte irredutível do sistema numérico, sendo a base de todos os números."(PERUZZO, 2012).

2.2 História

A primeira menção aos números primos de que temos conhecimento data de $6500a.C.$ e está em um osso, chamado osso de Ishango, que foi encontrado por Jean Heinzelin de Braucourt, um geólogo belga, na década de 1950. Hoje em dia, o osso de Ishango está exposto no Museu do Real Instituto de Ciências Naturais, na Bélgica. Esse osso aspresenta marcações em formato de linhas paralelas num total de 168 linha distribuídas em três colunas, essas linhas estão organizadas em grupos, mas de forma assimétrica, o que leva alguns pesquisadores a entender que suas distribuição não é meramente estética, mas com uma finalidade específica; por exemplo, em uma das colunas desse osso podemos observar 60 linhas separados em quatro grupos, o primeiro grupo possui 11 linhas, o segundo 13, o terceiro 17 e o quarto grupo possui 19 linhas (SANTOS, 2019). Essa separação em grupos contendo um número primos de linhas acontece em quase todo o osso.

Figura 1 – OSSO DE ISHANGO

No livro Elementos, de Euclides, datado de aproximadamente $300a.C.$, os números primos também são mencionados, além de resultados importantíssimos para seu estudo, como a prova da infinitude dos números primos e o Teorema Fundamental da Aritmética, que serão mencionados mais adiante.

A primeira tabela com os números primos foi feita pelo matemático grego Eratóstenes por volta do século III a.C., mais tarde, seu método foi chamado de Crivo de Eratóstenes, que é ensinado até hoje nas escolas. Esse método consiste em escrever todos

os números de 1 até um número desejado e limitado x, depois disso, excluímos o número 1, por não ser primo e nem composto, destacamos o número 2 por ser o primeiro primo e excluímos todos os seus múltiplos até x, dessa forma observamos o próximo número que não foi excluído, no caso, o número 3, destacamos ele e excluímos todos os seus múltiplos que ainda não tenham sido excluídos e repetimos esse processo com todos os números até x, os que não forem excluídos são números primos. Esse método é muito útil e simples quando estamos falando de números primos pequenos, mas não é muito eficaz para encontrar ou verificar números muito altos, de modo geral, encontrar e verificar a primalidade de números não é considerado algo simples, justamente pelo fato de os números primos não estarem apresentados de forma regular no conjunto dos números naturais.

Durante a Idade Média, assim como na maioria das áreas do conhecimento, a Matemática se estagnou e não houve grandes estudos ou descobertas, apenas no século $XVII$, com Pierre de Fermat que os números primos voltaram a ocupar a mente dos matemáticos, alguns como Euler e Gauss deram incríveis contribuições para o estudo dos números primos. Fermat, em seus estudos afirmou que todo número na forma $F_n = 2^{2^n} + 1$ era primo, esses números são conhecidos como números de Fermat, mas essa afirmação foi refutada por Euler em 1732 que mostrou que $F_5 = 2^{2^5} + 1 = 4.294.967.297$ não é primo, pois tem 641 e 6.700.417 como divisores. Gauss, por sua vez não tinha em mente descobrir quais eram os números primos, ele se ateve a descobrir a quantidade de números primos presente em determinado intervalo, a famosa fórmula $\pi(x)$ dos números primos, que diz quantos primos menores que x existem, ou seja, para todo $x \geq 0$ e $x \in \mathbb{N}$ definimos $\pi(x)$ como

$$\pi(x) = \{p \in \mathbb{N} | p \leq x\}$$

com p primo.

Gauss notou que para valores muito grandes de x

$$\pi(x) \approx \frac{x}{\ln x}$$

E a medida que o valor de x tendia ao infinito

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$$

Essa relação é conhecida como o Teorema dos Números Primos. (PERUZZO, 2012)

Até hoje não se sabe como os números primos estão distribuídos, não há ordem, não há método, não há lei de formação, função ou fórmula matemática que se saiba e que tenha validade para todos os números primos. E é exatamente essa falta de ordem que aflige, mas que ao mesmo tempo estasia os matemáticos de todos os tempos até a atualidade.

Como não foi encontrada uma forma de organizar os números primos, muitos estudiosos depositaram seus esforços em descobrir cada vez mais e mais primos, e cada vez maiores. As tábuas de números primos vêm sido escritas desde Eratóstenes e até hoje acrescentam números a essa tábua. Com o avanço da computação e da internet esse trabalho vem se tornando um pouco mais fácil, descobrindo cada vez mais primos e cada vez primos maiores. O maior primo descoberto até hoje é o número $2^{82589933} - 1$ com 24862048 dígitos, descoberto em 2019 por um projeto de pesquisa mundial chamado Great Internet Mersenne Prime Search (GIMPS), que se dedicam a descobrir os números primos da forma $2^n - 1$, conhecidos como primos de Mersene; e por mais que esse seja o maior número primo descoberto, não se sabe se todos os outros primos menores que ele são conhecidos, já que esse projeto se dedica a descobrir um tipo específico de números primos.

2.3 Resultados Importantes

Apesar de não se saber muito sobre sua disposição, os números primos possuem várias propriedades que auxiliam o estudo da Teoria dos Números, vamos destacar alguns desses resultados nessa seção.

Teorema 2.3.1 (Infinitude dos Números Primos)**.** *Existem infinitos números primos.*

Demonstração. (Euclides). Suponhamos que exista somente um número finito r de números primos, a saber $p_1, p_2, ..., p_r$. Consideremos agora o número $N = p_1 \cdot p_2 \cdot ... \cdot p_r + 1$. Se N for primo, então temos uma contradição, já que supomos existir somente r números primos e N evidentemente não é um deles. Se N não for primo, então existe um número primo p que divide N. Mas esse número primo p não pode ser nenhum dos números $p_i = (i = 1, ..., r)$, pois, se fosse, dividiria o produto $p_1 \cdot p_2 \cdot ... \cdot p_r$, e portanto dividiria o número 1, o que é um absurdo. Em ambos os casos, conclui-se a existência de mais números primos do que a quantidade suposta inicialmente. Logo, a suposição de que existe um número finito de números primos é falsa. □

Teorema 2.3.2 (Teorema Fundamental da Aritmética)**.** *Todo número natural n, com $n \geq 2$ ou é primo ou pode ser escrito como o produto de números primos de modo único, a menos de ordem.*

Demonstração. O teorema afirma que a decomposição de um número natural $n \geq 1$ em fatores primos existe, e é única (exceto pela ordem). Temos que provar, portanto, a existência e a unicidade desta decomposição.

Existência: se n for primo, ele é sua própria decomposição, a qual, portanto, existe. Suponhamos n composto. Tomemos $p_1 \geq 1$ o menor dos divisores naturais de n.

Temos que p_1 é primo, pois, caso contrário, existiria p natural ($1 \leq p \leq p_1$), com $p|p_1$ e portanto $p|n$, contradizendo a escolha de p_1. Assim, podemos escrever $n = p_1 \cdot n_1$.

Se n_1 for primo, novamente a prova está completa. Se n_1 é composto, tomemos p_2 como o menor fator de n_1. Pelo mesmo argumento, temos que p_2 é primo e portanto $n = p_1 \cdot p_2 \cdot n_2$. Se repetirmos esse procedimento obteremos uma sequência decrescente $n_1, n_2, ..., n_r$ de números naturais, todos maiores do que 1. Pelo Princípio da Boa Ordem, esse processo não pode continuar indefinidamente. Nesse momento teremos uma sequência $p_1, p_2, ..., p_k$ de números primos não necessariamente distintos. Logo, n terá a forma:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_l^{\alpha_l}$$

que é a decomposição de n em fatores primos.

Unicidade: a unicidade é mostrada usando indução sobre n. Para $n = 2$, a afirmação é verdadeira trivialmente. Assumimos que ela se verifica para todos os naturais maiores do que 1 e menores do que n. Vamos provar que ela também é válida para n.

Se n é primo, não há nada a provar. Suponhamos n composto, e que n possua duas decomposiçõees, ou seja,

$$n = p_1 \cdot p_2 \cdot ... \cdot p_s = q_1 \cdot q_2 \cdot ... \cdot q_r$$

onde os $p_i (i = 1, ..., s)$ e os $q_j (j = 1, ..., r)$ são números primos. Temos que provar que $s = r$ e que cada p_i é igual a algum q_j. Podemos escrever

$$p_2 \cdot ... \cdot p_s = \frac{q_1 \cdot q_2 \cdot ... \cdot q_r}{p_1}$$

e como o primeiro membro é um número natural, então $p_1|q_1 \cdot q_2 \cdot ... \cdot q_r$, o que implica que p_1 divide algum dos fatores q_j (que são todos primos). Sem perda de generalidade, podemos supor que $p_1|q_1$. Como ambos são primos, isto implica que $p_1 = q_1$. Logo:

$$1 \leq p_2 \cdot ... \cdot p_s = q_2 \cdot ... \cdot q_r \leq n$$

e aqui a hipótese de indução nos diz que as duas decomposições são idênticas, isto é, $s = r$ e, exceto pela ordem, as decomposições $p_1 \cdot p_2 \cdot ... \cdot p_s$ e $q_1 \cdot q_2 \cdot ... \cdot q_r$ são iguais. □

(SPENTHOF; SOUZA, 2013)

Esse teorema nos mostra que os números primos são a estrutura básica de todos os números naturais, são a partir deles que todos os números podem ser escritos de forma fatorada e única.

Muitos outros resultados podem ser citados como o Teorema dos Números Primos que foi mencionado na sessão anterior, o Lema de Euclides, o Pequeno Teorema de Fermat, o Teorema de Wilson, de Bertrand-Chebyshev, de Euler, o Postulado de Bertrand entre

outros. E ainda há outros problemas que estão em aberto como a Conjectura de Goldebach que diz que todo número natural, exceto o 2 pode ser escrito como a soma de dois números primos, e por mais que esse resultado tenha sido verificado para os números até 100 milhões, segue sem demonstração. (SPENTHOF; SOUZA, 2013)

2.4 Primos Especiais

Durante a busca de um padrão nos números primos, algumas das tentativas levaram os estudiosos a descobrirem certo subconjunto de primos que receberam nomes especiais, e por mais que ainda nunca se tenha achado a fórmula para todos, alguns merecem um certo destaque.

Os Primos de Fermat, que mencionamos anteriormente, são os primos da forma:

$$F_n = 2^{2^n} + 1$$

onde n é um número natural.

Mersene por sua vez, em seus estudos, também propôs uma fórmula para números primos, os primos de Mersene são da forma a seguir:

$$M_p = 2^p - 1$$

onde p é um número primo.

Maria Sophie Germain, uma matemática francesa, também deu sua contribuição, os primos de Sophie Germain são da forma,:

$$S_p = 2p + 1$$

onde p é um número primo

Os primos de Cullen, são todos primos da forma

$$C_n = n \cdot 2^n + 1$$

onde n é um número natural.

Outros que merecem destaque por suas características são os Primos Gêmeos, dizemos que dois primos são gêmeos quando a diferença entre eles é dois:

$$p, p + 2$$

com excessão do 2 e do 3, os primos nunca são números consecutivos, então a diferença entre números primos deve ser de no mínimo dois.

Quando a difereça entre dois primos é quatro, dizemos que eles são Primos Primos

$$p, p + 4$$

temos como exemplo de primos primos: 3 e 7, 7 e 11, 19 e 23, etc.

Podemos citar também os chamados Primos Fatoriais, que são os números primos na forma:

$$n! \pm 1$$

onde n é um número natural.

É importante lembrar que essas fórmulas não descrevem todos os números primos e que não são todos os números nesse formato que são primos, esse ainda é um mistério para todos os matemáticos. Então por que devemos aprender sobre os números primos? Qual a sua importância? Muitas vezes não vemos uma utilidade prática e diária de alguns conteúdos da Matemática, mas ela está inserida em nosso cotidiano mesmo que não possamos enxergá-la. Nesse trabalho vamos abordar um pouco onde os números primos são não só necessários, mas essenciais: a criptografia.

3 CRIPTOGRAFIA

Todos presamos pelo sigilo das nossas informações pessoais desde muito cedo, a privacidade sempre foi algo importante para o ser humano. Crescemos e nos deparamos com senhas, contas bancárias, entre outras informações que sabemos que são confidenciais, mas como é possível guardar todas essas informações, sem que não caia "em mãos erradas"?

3.1 Definições

A palavra criptografia vem do grego *kriptos* que significa oculto, escondido e *grifo* que significa grafia, escrita. Foi muito utilizada nos períodos de guerra para que mensagens fossem transmitidas as tropas aliadas e que, se fossem interceptadas no meio do caminho, não pudessem ser lidas por tropas inimigas. Mas existem formas diferentes de se esconder essa mensagem, de ocultar seu significado e principalmente de "traduzir"a mensagem secreta. Para esse fim, vamos definir a diferença entre esses termos para que a compreenção seja um pouco maior.

Definição 3.1.1 (Esteganografia)**.** É a arte de camuflar uma mensagem, escondê-la fisicamente, para que não se descubra sua existência.

Quando escondemos nossas informações em baixo do colchão, colocamos nossas senhas dentro de um cofre, essa informação está protegida, está oculta, escondida daqueles que não necessitam da informação. Quando a tecnologia não era desenvolvida como é hoje, mensagens secretas eram mandadas de forma escondida, o historiador Heródoto conta a história de determinado escravo que teve uma mensagem escrita em seu coro cabeludo, cujo cabelo foi previamente raspado, depois que o cabelo cresceu, ele foi mandado ao seu destino passando despercebido pelos guardas que verificaram suas roupas e bagagens, mas não viram a mensagem por debaixo dos seus cabelos, quando chegou, bastava raspar seu cabelo mais uma vez e a mensagem chegaria ao seu destinatário, (ALVARENGA, 2017, p. 05). Mas perceberam que só ocultar fisicamente a mensagem não era muito seguro, via-se então a necessidade de ocultar também a mensagem escrita, caso o esconderijo fosse descoberto.

Definição 3.1.2 (Criptografia)**.** É o conjunto de regras e técnicas que permitem ocultar o significado de uma mensagem de todos aqueles que não sejam os legítimos receptores da mesma, a partir de uma convenção combinada de como essa mensagem seria “traduzida”.

A palavra criptografia vem do grego *kriptos* que significa oculto, escondido e *grifo* que significa grafia, escrita. Logo podemos entender que a criptografia é uma escrita oculta,

secreta. O processo de criptografia está ligado ao codificar, que consiste em transformar a mensagem original em uma mensagem secreta através de um código ou regra que também pode ser chamada de chave que identifica todos os detalhes para fazer essa mudança, e decodificar a mensagem, que significa transcrever a mensagem de volta para a original. Podemos estabelecer uma diferença aqui entre decodificar e decifrar, decodificar significa que a mensagem é para você e você sabe o código pois ele já foi pré-estabelecido; decifrar está mais ligado a você descobrir a regra, por outros meios, ou seja, a mensagem não era para você, mas você conseguiu quebrar o código dela para acessá-la, através dessa informação podemos definir o que é Criptoanálise.

Definição 3.1.3 (Criptoanálise)**.** É a parte que se dedica a decifrar os códigos que são estabelecidos, seja por força bruta (tentando todas as possibilidades), por lógica ou com a ajuda de computadores.

Enquanto uns se dedicam a desenvolver sistemas para criptografar mensagens, outros se dedicam a descobrir fraquezas nesses sistemas, para que a mensagem seja decodificada. Nenhum sistema é perfeitamente seguro, todos tem uma falha, e a criptoanálise existe para descobrir essa falha ou pelo menos diminuir sua eficiência. Veremos mais adiante como todos os sistemas antigos foram decifrados e como se tornaram obsoletos para os dias atuais.

Definição 3.1.4 (Criptologia)**.** é como chamamos a junção da criptografia e da criptoanálise, estudando tanto a forma de codificar e decifrar um código como também a forma de quebrá-lo.

3.2 Criptografia de Substituição

Um exemplo de criptografia que foi muito usada na antiguidade foi a criptografia de substituição, que consiste em substituir as letras e números da mensagem por símbolos ou até mesmo por outras letras em sequências diferentes. O imperador César foi o primeiro, que se tem notícia, a usar essa substituição das letras do alfabeto, ele trocava cada letra pela terceira letra a sua frente. Por exemplo, a letra A era trocada pela letra D, B por E, e assim até que as últimas letras do alfabeto fossem trocadas pelas primeiras, por esse motivo, esse tipo de criptografia é chamado de Cifra de César.

Por exemplo, se quiséssemos criptografar a mensagem:

MATEMÁTICA É A MELHOR MATÉRIA

com a substituição de César, a mensagem criptografada seria:

PDWHPDWLFD H D PHOKRU PDWHULD

Podemos também citar o Código Maçônico, que também consistia em trocar as letrar do alfabeto por símbolos pré-estabelecidos pelos maçons, além do Código Morse, muito conhecido também, onde cada letra do alfabeto é trocada por um conjunto de pontos e traços e que foi muito usado no período do telégrafo, para mandar e receber mensagens.

Todos esses exemplos a troca era feita um-a-um, mas existia uma variação desse tipo de criptografia onde uma letra era trocada por um par, ou conjunto de letras definido como uma substituição polialfabética. A *Cifra de Vigenere* é um exemplo famoso de criptografia polialfabética, em resumo ela funcionava como um plano cartesiano, onde as letras eram substituídas por pares de letras organizadas em linhas e colunas.

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

Figura 2 – CIFRA DE VIGENERE

Existia várias variações da cifra, onde as letras suporte eram trocadas de lugar ou substituídas por números, ou até mesmo um pouco dos dois.

Entretanto esses métodos eram pouco eficazes pois a frequência que uma letra é usada em determinada língua é por vezes constante e facilmente descoberta, vários sites da internet já disponibilizam esse tipo de informação, podendo até mesmo ser deduzida a partir de um texto, consideravelmente longo na mesma língua, observando essa frequência e aplicando no texto criptografado. Segundo o site Só História, o objeto mais famoso que contém esse tipo de criptografia é a Pedra de Roseta, que foi descoberta em 1799 em uma expedição militar de Napoleão Bonaparte e que foi decifrada em 1822 por um estudante francês chamado Jean-François Champollion, hoje ela se encontra no Museu Britânico em Londres. Nesse bloco existe a mesma mensagem escrita em hieróglifos, demótico e grego.

3.3 Criptografia de Transposição

Outro exemplo é a criptografia de transposição, onde se usa as mesmas letras, só que rearranjadas, formando anagramas. Para palavras ou frases curtas esse processo se

torna muito simples de ser decodificado ou decifrado, o que impossibilita seu uso. Para mensagens muito grandes se torna inviável pois a quantidade de possíveis soluções é exorbitante, deixando extremamente complicado até mesmo para a pessoa que deverá receber a mensagem. Uma variação desse método de criptografia é a *Cerca de Ferrovia* que consiste em escrever as letras alternadas em linhas diferentes e depois usar a sequência formada nas linhas, nessa nova ordem.

O primeiro aparelho criptográfico que foi utilizado para esse tipo de criptografia foi o *Citale Espartano*, era um objeto de formato cilíndrico onde se enrolava uma fita de couro ou de pergaminho. A mensagem era escrita na fita enrolada, e para que o receptor pudesse ler a mensagem era necessário um objeto semelhante que possuísse o mesmo diâmetro.

Figura 3 – CITALE ESPARTANO

Um outro instrumento utilizado para esse tipo de criptografia foi o *Disco de Alberti* que consistia em dois círculos concêntricos de diâmetros diferentes, presos por um pino central, com o círculo de diâmetro menor podendo ser girado. Os dois discos eram divididos em 24 setores contendo 20 das letras do alfabeto e os números 1, 2, 3 e 4. De maneira bem resumida, a forma como a mensagem era criptografada e decodificada dependia da posição estabelecida entre as letras do círculo menor (mensagem criptografada) em relação as letras do círculo maior (mensagem original).

Mas esses processos de criptografia não eram muito confiáveis, pois existia a dependência desses instrumentos, além de que eles poderiam ser perdidos, recriados ou até mesmo cair em mãos erradas.

3.4 Criptografia Assimétrica

Os exemplos dados acima são chamadas de criptografias simétricas que significa que a chave usada para criptografar a mensagem era a mesma usada para decodificá-la, seja ela uma regra ou um instrumento, então essa chave era única e deveria ser conhecida apenas por quem escreveu a mensagem e por quem deverá recebe-la, mas isso trouxe dois problemas significativos, o primeiro era a disponibilização dessa chave apenas para as pessoas certas, o outro problema consistia em caso essa chave se tornasse pública ou fosse descoberta, a mensagem seria decodificada muito facilmente e por qualquer um, e poderia

até mesmo ser modificada, reescrita, passando dados e informações erradas, se passando por certas. Singh (2004, p. 28) foi muito enfático ao colocar:

> "A importância da chave, em oposição ao algoritmo é um princípio constante da criptografia, como foi definido de modo definitivo em 1883 pelo linguista holandês Auguste Kerckhoff, em seu livro *La Cryptographie Militaire*. Este é o Princípio de Kerckhoff: ' A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave.'" (SINGH, 2004)

A partir dessa visão, foi desenvolvida a criptografia assimétrica, ou criptografia de chave pública. Ela se baseia não apenas em uma chave, como a criptografia simétrica, mas em duas chaves: uma pública e uma privada. A chave pública é usada para codificar a mensagem a ser enviada e a chave privada para decodificá-la, como o acesso a essa chave privada é restrito, as chances de a mensagem ser decifrada são mínimas. As pessoas podem até descobrir como criptografar a mensagem, mas isso não ajudaria na hora de decodificá-la, pois não funciona como a criptografia simétrica.

> "A criptografia de chave pública utiliza duas chaves, que são relacionadas matematicamente e construídas para trabalharem juntas. Uma das chaves do par é dita a chave privada (pessoal) e é mantida em segredo, sendo conhecida apenas pelo dono do par de chaves. A outra chave do par é dita a chave pública, porque é conhecida publicamente."(BRAGA; DAHAB, 2018)

Dessa forma, aquele que precisa receber a mensagem divulga a chave publica, e mantém com ele a chave privada, dessa forma qualquer um pode mandar uma mensagem criptografada para ele, mas apenas ele pode decodificar essa mensagem, pois só ele possui a chave de decodificação.

Existem várias criptografias assimétricas, as mais famosas são a criptografia RSA, que receberá uma atenção especial nesse trabalho, acordos de chaves com Diffie-Hellman (DH), Criptografia de Curvas Elípticas (Elliptic Curve Cryptography - ECC), distribuição de chaves públicas com certificação digital e noções gerais sobre o protocolo Transport Layer Security (TLS).Braga & Dahab (2018, p.52)

3.5 História

Nessa sessão usamos o livro (ALVARENGA, 2017) como referencial teórico para as informações históricas.

3.5.1 Idade Antiga

Como já mencionado, o primeiro tipo de criptografia foi a de substituição, o que podemos chamar de uma criptografia ingênua, pela facilidade de decodificá-la, os povos egípcios, gregos, romanos e hebreus são exemplos do uso desse tipo de criptografia, que por mais simples, era suficiente para a época.

Vale relembrar que a criptografia não era de uso exclusivamente militar, os hebreus por exemplo, usavam a criptografia para escrever seus textos religiosos, o mais conhecido é o *Atabash*, que consistia em trocar a primeira letra do alfabeto hebraico pela última, a segunda pela penúltima, e assim por diante. A arte também fez uso da criptografia, além de mensagens pessoais e privadas, sem o intuito bélico.

3.5.2 Idade Média

Com o avanço da criptoanálise e a percepção da frequência das letras em cada língua, muito se foi pensado, desde acrescentar letras e palavras aleatórias ao texto, até deixar pré-estabelecido a ausência de uma das letras de propósito, para que a decodificação se tornasse mais difícil, o que deu certo por um curto período de tempo, mas logo foi quebrado também, entrando em desuso.

Algum tempo depois, principalmente no império islâmico-árabe, durante a Idade Média e a Renascença, a criptografia foi se desenvolvendo, devido à expanção desse império, a necessidade do avanço político-militar indispensável para o governo na época, principalmente no que diz respeito ao envio e recebimento de mensagens privadas. (ALVARENGA, 2017, p. 47)

Ibn Dunainir ou Ibrahim Ibn Mohammad ibn Dunainir (1187-1229) foi o introdutor das cifras algébricas, onde as letras eram substituídas por números e operações aritméticas eram usadas para criptografar a mensagem. Ibn Ad-Duraihim (1312 – 1361) fez muitas contribuições para essa área também, em um dos seus livros, *Miftah al-Kunuz fi Idah al-Marmuz* (Chaves para a Elucidação de Mensagens Secretas) ele aborda e organiza a classificação das cifras até então conhecidas, a análise da frequência das letras em várias línguas e tabelas de encriptação polialfabética, como a de *Vigenere* e grades de transposição.

Enquanto isso a Europa vivia seus dias nas trevas do conhecimento, onde a criptografia era considerada bruxaria, ficando bem atrás dos avanços árabes. Até que durante o Renacimento o cenário começou a mudar. Um de seus precursores foi Leone Battista Alberti, que em 1404, utilizando a criptografia de substituição poliafabética, inventou a primeira máquina de criptografia assistida, o Disco de Alberti, já mencionado anteriormente.

Uma cifra que merece reconhecimento é a dos Cavaleiros Templários, organização

que foi fundada no ano de 1118 e tinha como objetivo proteger os peregrinos que estavam a caminho da Terra Santa, essa organização cresceu exponencialmente por todo o mundo, vendo-se a necessidade de uma comunicação segura e sigilosa. Sua sifra era de substituição simples, o que era inovador na Europa, mas de fácil decifração na arábia.

3.5.3 Idade Moderna

Mas a cada mensagem decodificada, via-se a necessidade do melhoramento dos métodos de criptografia, e a cada mensagem criptografada via-se a necessidade do avanço da quebra desses códigos. Máquinas foram criadas exclusivamente para criptografar e decodificar mensagens, podemos citar por exemplo o Disco de Cifras de Thomas Jefferson, criada em 1795; a Enigma do polonês Arthur Scherbius, criada no fim da Primeira Guerra Mundial, em 1918 e que foi muito utilizada durante a Segunda Guerra Mundial, além de uma máquina japonesa muito famosa chamada *Purple Machine*, entre outras. Essas máquinas se tornaram cada vez mais comuns em diversos países, eram programadas para codificarem o texto por substituições polialfabéticas das mais variadas maneiras de acordo com o que seu dono colocasse como informação.

Figura 4 – DISCO DE CIFRAS DE THOMAS JEFFERSON

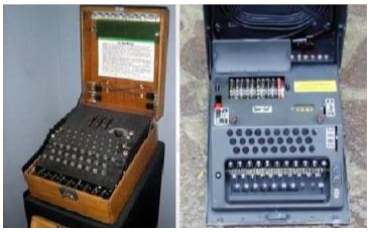

Figura 5 – ENIGMA

Figura 6 – PURPLE MACHINE

Estudos foram feitos e equipes inteiras foram formadas para pensarem em algo novo a fim de que houvesse esse sigilo e essa segurança em mandar e receber mensagens e dados, os governos começaram a procurar e contratar pessoas que tinham essas habilidades, tanto para pensarem em novas cifras, como para quebrar as cifras já existentes. A Inteligência Militar contava agora com um novo grupo, que não estava à frente da batalha, mas que eram tão essenciais quanto.

3.5.4 Idade Contemporânea

Com o avanço da tecnologia e da comunicação via internet, interceptar essas mensagens se tornou consideravelmente simples, então o foco não era, necessariamente, esconder a existência da mensagem, e sim o conteúdo que ela continha. Dessa forma a criptologia também viu a necessiade de avanço, as máquinas criadas pós Primeira Guerra já não eram tão confiáveis assim, as cifras de substituição polialfabética se tornaram tão evidentes que qualquer computador poderia decifrá-la facilmente, um novo desafio foi dado à essa ciência: a criação de uma cifra que não dependesse apenas da substituição e que fosse legível para seus receptores.

Dessa forma as criptografias assimétricas ganharam seu espaço, já que a chave para a decodificação não é divulgada e nem necessária, a não ser para aquele que recebe a mensagem, e o fato de a chave para a encriptação ser pública e qualquer um ter acesso a ela e poder mandar uma mensagem encriptografada facilita no envio da mensagem e dificulta o trabalho dos criptoanalistas que precisam decifrar a mensagem.

Hoje a criptografia também é usada para enviar e receber dados pessoais e empresariais, transações bancárias, compras com cartão de crédito via internet. Esse tipo de conteúdo, se divulgado, pode comprometer a dignidade pessoal e financeira da pessoa ou empresa envolvidas; então a mensagem enviada precisa ser ilegível para qualquer concorrente ou ladrão, mas também precisa ser clara para aquele a quem a mensagem é destinada, para que não haja confusão nas informações.

4 CÓDIGOS E NÚMEROS PRIMOS

Falamos sobre os números primos e sobre criptografia nesse trabalho, nesse capítulo vamos mostrar qual a interação entre esses dois assuntos e como eles se relacionam para manter o sigilo entre informações.

4.1 Necessidade

Como já mencionado, na criptografia simétrica, a forma como a mensagem é criptografada é a mesma como ela é descriptografada, então esse método deve ser conhecido tanto pelo emissor da mensagem quanto pelo receptor da mesma. Mas com os avanços tecnológicos a maioria das trocas de informações são feitos via internet, logo se o método é divulgado, a mensagem pode facilmente ser deciptografada, ou até mesmo modificada por terceiros.

Qaundo compramos produtos pelo cartão de crédito, por exemplo, informamos os dados do cartão, se esses dados forem interceptados e descobertos, isso poderia comprometer o sigilo financeiro do comprador, dessa forma percebeu-se que as criptografias simétricas não eram mais funcionais na era tecnológica, abrindo espaços para a criptografia assimétrica.

> "Para cifrar a mensagem secreta ele (remetente) deve usar uma chave, também secreta, daí surge o problema de transmitir uma chave secreta para o receptor de modo a poder transmitir a mensagem secreta. Resumindo, antes que duas pessoas possam partilhar um segredo (mensagem cifrada), elas devem antes partilhar outro segredo (a chave)."(SINGH, 2004)

Então como manter essa chave em segredo? A criptografia assimétrica auxiliou nesse sentido, pois não há necessidade de partilhar a chave com ninguém. De forma bem grosseira, podemos explicar a criptografia assimétrica dessa forma: é como se o receptor da mensagem distribuísse vários cadeados iguais, ou seja, todos que desejassem mandar uma mensagem secreta para ele bastava escrevê-la e ”trancá-la” com um desses cadeados, qualquer um pode escrever e mandar a mensagem, mesmo não tento contato direto com o receptor e qualquer um poderia interceptar a mensagem e ver que ela está ”rancada” com esse cadeado, mas o único que pode ”abrir” o cadeado e ler a mensagem é quem tem a chave, essa chave está nas mão dos receptor e não foi, nem deveria, ser divulgada a público.(SINGH, 2004, p. 296)

4.2 Método RSA

O método de chave pública mais conhecido é o RSA. Que foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época eram pesquisadores no Laboratório de Ciências da Computação no *Massachussets Institute of Technology* (MIT). O nome RSA é referente a inicial dos nomes dos seus criadores. Existem outras formas de criptografia de chave pública, mas a mais usada e que será mais abordada nesse trabalho é a RSA.

4.2.1 Pré-Codificação

Para criptografar uma mensagem em RSA, primeiramente devemos dividir a mensagem em blocos de tamanho fixo. Através de uma pré-codificação, esses blocos são transformados em uma sequência numérica. Podemos usar uma substituição simples para essa pré-codificação inicial, por exemplo, substituir A por 10, B por 11 e assim por diante, é interessante começarmos por 10 para que não haja problema de interpretação, pois se começarmos substituindo A por 1, o número 12 poderia ser interpretado pela letra L, ou pelas letras AB em sequência. Devemos também ter um valor para os espaços e para os números de 1 a 9, caso seja necessário na mensagem. Concordamos com CARNEIRO (2017, p.79) quando afirma:

> "Criptografar uma mensagem significa aplicar uma função f à sequência de números. Decifrar a mensagem consiste em aplicar a função inversa $g = f^{-1}$. A questão toda é encontrar a função f tal que seja inviável para um atacante encontrar sua inversa f^{-1}. "(CARNEIRO, 2017)

4.2.2 Codificação

Partindo desse princípio que Rivest, Shamir e Adleman desenvolveram seu método. Depois da pré-codificação devemos escolher os parâmetros RSA que são dois primos distintos, vamos chamar esses dois primos de p e q. A partir deles, calculamos seu produto $n = p \cdot q$ que é chamado de módulo RSA. Depois de escolhidos os parâmetros e encontrado o módulo devemos separar a mensagem pré-codificada em blocos, essa separação deve ser feita de maneira aleatória, mas deve-se observar três aspectos: o bloco não pode formar um número maior que n (o módulo RSA), o bloco não pode começar por 0 (devido a possíveis confusões na decodificação) e o bloco não deve corresponder a uma palavra ou letra específicos (para que a decodificação por contagem de frequência seja impossível).

Vamos denotar por $\phi(n) = (p-1)(q-1)$, vamos precisar desse valor para o próximo passo da criptografia RSA. Para codificar a mensagem devemos encontrar um inteiro positivo, que chamaremos de x, de modo que o $m.d.c.(x, \phi(n)) = 1$. O par (n, x) é

o que chamamos de chave pública da criptografia RSA. Esse par de números é divulgado, qualquer um pode ter acesso a ele para mandar mensagens criptografadas.

A mensagem que estava em uma única sequência numérica foi separada em blocos menores que chamaremos de b, vamos codificar cada um desses blocos separadamente e deixar separado depois de codificado, pois se unirmos seria impossível voltarmos a mensagem original. Para codificarmos cada bloco devemos calcular b^x e o novo bloco será formado pelo resto da divisão desse valor por n.

Dessa forma teremos uma nova sequência de blocos, onde cada um dos blocos é representado pelo resto da divisão de b^x por n, chamaremos cada um desses novos blocos de a, que contém a mensagem codificada.

4.2.3 Decodificação

Para decodificar a mensagem precisamos de dois números n e y, tal que o produto $y \cdot x$ deixe resto 1 na divisão por $\phi(n)$. Assim, o par (n, y) é a chamada chave privada da criptografia RSA.Para realizarmos a decodificação devemos calcular a^y e verificar qual o resto da divisão dele por n. Os blocos encontrados quando fazemos a^y serão exatamente os blocos que foram originalmente separados no começo da codificação.

Pensando dessa forma, a decodificação parece ser bem simples, e em teoria realmente é, desde que saibamos calcular o valor de $\phi(n)$, mas para calcularmos seu valor é necessário saber a fatoração de n, como os números p e q não são divulgados, temos então de usar recursos matemáticos para realizar essa fatoração. Quando falamos de números pequenos, fatorá-los não é uma tarefa tão complicada assim, mas se estamos falando de números muito grandes, até mesmo computadores superpotentes demorariam algumas centenas de anos para fatorá-lo.

4.2.4 Exemplo

Vamos criptografar a palavra PROFMAT usando a criptografia RSA. Para isso, devemos usar uma pré-codificação que funcionará da seguinte forma:

Dessa forma a palavra PROFMAT pode ser pré-codificada por:

$$25272415221029$$

Para facilitar o processo, vamos escolher os parâmetros RSA pequenos, no caso $p = 3$ e $q = 11$, mas vale lembrar que na codificação usual, os primos escolhidos tem muito mais dígitos. A partir dessa escolha teremos que $n = p \cdot q = 3 \cdot 11 = 33$, será nosso módulo RSA.

Tabela 1 – PRÉ-CODIFICAÇÃO RSA.

LETRA	**NÚMERO**	**LETRA**	**NÚMERO**	**LETRA**	**NÚMERO**
A	10	J	19	S	28
B	11	K	20	T	29
C	12	L	21	U	30
D	13	M	22	V	31
E	14	N	23	X	32
F	15	O	24	W	33
G	16	P	25	Y	34
H	17	Q	26	Z	35
I	18	R	27		99

Fonte: Produzida pelos autores

Calculando $\phi(x) = (p-1)\cdot(q-1) = (3-1)\cdot(11-1) = 2\cdot 10 = 20$, a partir disso escolhemos um inteiro x tal que $m.d.c.(x, \phi(n)) = 1$, no caso, vamos escolher $x = 7$, pois $m.d.c(7, 20) = 1$.

Dessa forma nossa chave pública será $(33, 7)$.

Então vamos pegar o nosso código e separar em blocos de modo aleatório, importante lembrar que cada bloco que separamos na pré-codificação seja menor que o nosso módulo RSA, uma das formas possíveis é:

25 27 24 15 22 10 29

O ideal é que cada bloco não represente uma letra ou uma palavra, para dificultar a decodificação, mas para simplificar as contas faremos a codificação por letras, uma outra forma de se fazer a codificação é número por número, que funciona também.

Para codificar os blocos, devemos elevar cada número a 7 e verificar qual o resto da divisão desse valor por 33:

Tabela 2 – CODIFICAÇÃO RSA.

b	b^7	**RESTO DA DIVISÃO**
25	6103515625	31
27	10460353203	3
24	4586471424	18
15	170859375	27
22	2494357888	22
10	10000000	10
29	17249876309	17

Fonte: Produzida pelos autores

Dessa forma, a nossa nova sequência, agora codificada, será:

31 3 18 27 22 10 17

Para decodificar nossa mensagem precisamos de um valor y que quando multiplicado por 7 deixe resto 1 na divisão por 20. O menor valor possível para y é 3. Pois $3 \cdot 7 = 21$ que deixa resto 1 na divisão por 20. Um outro valor possível seria o 23, pois $23 \cdot 7 = 61$, que também deixa resto 1 na divisão por 20. Usaremos o 3 para facilitar os cálculos.

Na decodificação, devemos pegar os blocos formados na codificação, elevar cada bloco a $y = 3$ e verificar qual o resto da divisão dessa potência por 33:

Tabela 3 – DECODIFICAÇÃO RSA.

a	a^3	**RESTO DA DIVISÃO**
31	29791	25
3	27	27
18	5832	24
27	19683	15
22	10648	22
10	100	10
17	4913	29

Fonte: Produzida pelos autores

Voltando ao código inicial, que revendo a Tabela 1 podemos decodificar a mensagem:

25 27 24 15 22 10 29

de volta para PROFMAT, através de uma substituição simples.

Perceba que y foi facilmente encontrado pois o valor público 21 é fácil de ser fatorado, deixando simples o cálculo de $\phi(n)$, mas isso não é tão simples para valores muito altos.

4.3 Segurança do método

Esse processo pode parecer bem simples, como já mencionado, mas encontrar esse valor de y sem sabermos os valores de p e q é um processo extremamente demorado, principalmente se esses valores forem extremamente altos.

Isso não significa que esse método é inquebrável, significa que enquanto não acharem uma forma mais rápida de se fatorar um número consideravelmente grande, o método continua sendo eficaz, isso pode acontecer em algumas décadas ou até mesmo amanhã. Muitos matemáticos tentaram achar atalhos para a fatoração, mas não obtiveram sucesso, a fatoração continua sendo um processo árduo e trabalhoso para todos aqueles que necessitam dela.

Na Tabela 4, mostraremos o tempo necessário para se fatorar um número levando em consideração a quantidade de dígitos que o número possui no sistema decimal e a

quantidade de operações matemáticas necessárias para que isso ocorra. Esses dados são trazidos pelos próprios autores do método RSA de criptografia em um dos seus trabalhos Rivest, Shamir & Adleman (1978, p.12)

Tabela 4 – Tempo estimado para a fatoração de um número

Dígitos que o número possui	Quantidade de operações matemáticas necessárias	Tempo estimado
50	$1,4 \cdot 10^{10}$	3,9 horas
75	$9,0 \cdot 10^{12}$	104 dias
100	$2,3 \cdot 10^{15}$	74 anos
200	$1,2 \cdot 10^{23}$	$3,8 \cdot 10^{9}$ anos
300	$1,5 \cdot 10^{29}$	$4,9 \cdot 10^{15}$ anos
500	$1,3 \cdot 10^{39}$	$4,2 \cdot 10^{25}$ anos

Fonte: (RIVEST; SHAMIR; ADLEMAN, 1978)

Nessa tabela, o maior número possui 500 dígitos, mas no final da Sessão 2.2 foi comentado que o maior primo que temos conhecimento possui 24862048 dígitos, podemos então perceber que o método RSA é bem seguro, e mesmo com computadores superpotentes, ainda teremos um bom tempo de espera para quebrar o código.

Observamos tabém que pelo fato de os números primos serem infinitos, a criptografia RSA sempre terá material para usar, fora que descobrir a primalidade de um número é muito mais fácil que fatorá-lo. Para se ter uma noção, sabe-se que $2^{2^{14}} + 1$ é composto, mas não sabemos nenhum dos seus fatores (COUTINHO, 1997, p.5). Isso acontece por que verificar a primalidade de um número não está intimamente ligada a fatorá-lo, muitas propriedades só são válidas para números primos, como os mencionados no fim da Sessão 2.3.

5 Considerações finais

As tecnologias se renovam todos os dias, podemos perceber que as pessoas estão cada vez mais dependentes da internet e do que ela oferece. Dessa forma é importante que se tenha o conhecimento necessário para saber como ela funciona. Num espaço onde todos tem livre acesso devemos nos preocupar com nossas informações pessoais, nosso sigilo e privacidade, nem tudo o que postamos é público, algumas coisas são particulares.

Como as tecnologias estão presentes no nosso cotidiano, devemos entender os processos que ela utiliza, a criptografia está presente em todas as nossas compras online, nas mensagens de texto eletrônicas, em informações de aplicativos de *streaming*. Para a nossa segunça, a criptografia RSA transforma todas essas informações em códigos que, a princípio, são ilegíveis para todos aqueles que tentarem interceptar essas informações, e isso acontece graças as dificuldades que os computadores tem em fatorar números inteiros em fatores primos.

Conhecer os números primos e suas propriedades levaram a criptografia onde ela está hoje, graças a essas propriedades, hoje temos um método onde a chave de codificação é pública e qualquer um que pode codificar uma mensagem, mas onde a chave de decodificação é privada, aumentando ainda mais a segurança dos nossos dados online.

Muitos matemáticos ainda se dedicam a encontrar uma fórmula de fatorar números primos mais rápida e simples, esse é um problema real e em aberto. Muitos resultados e conjecturas relacionados aos números primos também estão em aberto, como os citados no capítulo de números primos. Além da grande incógnita que é encontrar um padrão na distribuição dos números primos nos números naturais, assunto que assombra os matemáticos há séculos.

Acreditamos que esse trabalho pode trazer uma ampliação nos horizontes, no que diz respeito à comunicação, números primos, criptografia e suas relações. Desde a necessidade que o ser humano tem em se comunicar, até a necessidade dessa comunicação, em diversas vezes, ser privada e restrita a um indíviduo ou um grupo específico. A evolução da criptografia usando números primos é algo real e cotidiano, mesmo não que não vejamos isso de maneira direta, conhecer como funciona essa codificação das nossas mensagens pode nos trazer segurança na hora de compartilharmos informações.

Referências

ALVARENGA, L. G. D. **Criptografia Clássica E Moderna**. [S.l.]: Clube de Autores (managed), 2017. Citado 3 vezes nas páginas 25, 29 e 30.

BRAGA, A.; DAHAB, R. Criptografia assimétrica para programadores-evitando outros maus usos da criptografia em sistemas de software. **Caderno de minicursos do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais—SBSeg**, v. 2018, p. 1–50, 2018. Citado na página 29.

CARNEIRO, F. J. F. **Criptografia e Teoria dos Números**. 2017. Citado na página 34.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. [S.l.]: IMPA, 1997. Citado na página 38.

EDUCAÇÃO, B. M. da. **Base Nacional Comum Curricular**. [S.l.]: MEC/CONSED/UNDIME, 2017. Citado na página 17.

LARUCCIA, M. M. Notas sobre linguagem, comunicação e educação. **Pensamento & Realidade**, v. 15, 2004. Citado 2 vezes nas páginas 15 e 16.

NACIONAIS, I. A. P. C. terceiro e quarto ciclos do ensino fundamental. **Brasília: MEC-Secretaria de Educação Fundamental**, 1998. Citado na página 14.

PARTE, I. Linguagens, códigos e suas tecnologias. **Brasília: MEC**, 2000. Citado na página 16.

PERUZZO, J. **O Fascínio Dos Números Primos**. [S.l.]: Clube de Autores (managed), 2012. Citado 2 vezes nas páginas 18 e 20.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. **A method for obtaining digital signatures and public-key cryptosystems**. [S.l.]: ACM New York, NY, USA, 1978. 120–126 p. Citado na página 38.

SANTOS, C. Os números primos de ishango. **Revista Brasileira Multidisciplinar**, v. 22, n. 2, p. 120–130, 2019. Citado na página 19.

SINGH, S. **O livro dos códigos**. [S.l.]: Editora Record, 2004. Citado 3 vezes nas páginas 14, 29 e 33.

SPENTHOF, R. L.; SOUZA, J. A. de. Primos: Da aleatoriedade ao padrao. **Revista Eletrônica da Sociedade Brasileira de Matemática. Rio de Janeiro**, v. 1, n. 1, 2013. Citado 2 vezes nas páginas 22 e 23.

TECNOLÓGICA, B. S. de Educação Média e. **Parâmetros curriculares nacionais: ensino médio**. [S.l.]: MEC, 1999. Citado na página 17.