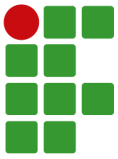


INSTITUTO FEDERAL
Brasília
Campus Estrutural

Instituto Federal de Brasília *Campus* Estrutural
Licenciatura em Matemática

GUILHERME GUIMARÃES DE MIRANDA

CRIPTOGRAFIA RSA

BRASÍLIA

JULHO/2022

GUILHERME GUIMARÃES DE MIRANDA

Criptografia RSA

Trabalho de conclusão de curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia de Brasília Campus Estrutural como parte dos requisitos necessários à obtenção do título de Licenciado em Matemática.

Orientador: Vinicius Facó Ventura Vireira

Brasília

Julho/2022

Dados da Catalogação na Publicação
Elaboração Walison A. Oliveira CRB1-3477

M672c Miranda, Guilherme Guimarães

Criptografia RSA [recurso eletrônico] / Guilherme Guimarães. 2022.
Dados eletrônicos (1 arquivo : 60 páginas.: il.; 21 cm).

Orientador: Prof. Dr. Vinicius Facó Ventura Vieira.

Trabalho de Conclusão de Curso (graduação) - Instituto Federal de Educação, Ciência e Tecnologia de Brasília, Campus Estrutural, Curso de Licenciatura em Matemática, Brasília, 2022.

Bibliografia: p. 59-60.

1. Criptografia. 2. Matemática - Estudo e ensino. 3. Teoria dos números. 4. Números primos. I. Vieira, Vinicius Facó Ventura, orient.. II. Título. III. Instituto Federal de Educação, Ciência e Tecnologia de Brasília.

CDU: 004.056:511:37

MINISTÉRIO DA EDUCAÇÃO
Instituto Federal de Educação, Ciência e Tecnologia de Brasília

FICHA DE APROVAÇÃO EM BANCA EXAMINADORA

Trabalho de Conclusão de Curso

Discente: Guilherme Guimarães de Miranda
Título: CRIPTOGRAFIA RSA.

Trabalho apresentado ao curso de Licenciatura em Matemática do Campus Estrutural do Instituto Federal de Brasília como requisito parcial para a obtenção de título de Licenciado em Matemática.

Trabalho aprovado em: 28/07/ 2022.

Brasília - DF, 28 de Julho de 2022.

Banca Examinadora

Orientadora (Presidente): Prof.º Dr. Vinícius Facó Ventura Vieira
Examinador (1º membro): Prof.º Dr. Jorge Augusto Gonçalo de Brito.
Examinador (2º membro): Prof.ª Ma. Juliana Campos Sabino de Souza.

Documento assinado eletronicamente por:

- **Juliana Campos Sabino de Souza**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 03/08/2022 17:37:55.
- **Jorge Augusto Goncalo de Brito**, **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 28/07/2022 21:32:50.
- **Vinicius Faco Ventura Vieira** , **PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 28/07/2022 20:37:06.

Este documento foi emitido pelo SUAP em 28/07/2022. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifb.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 397655
Código de Autenticação: 6b5dd8bea8

Agradecimentos

Agradeço primeiramente a Deus, pelo amor, misericórdia e toda a força que me foi me dada, sempre nos momentos em que mais precisei.

Agradeço aos meus pais, Edna Maria Guimarães de Miranda e Francisco Assis Guida de Miranda (in memoriam), que acreditaram e me deram apoio, em 2019, para trocar de curso e seguir minha vontade de fazer Matemática. Além de cada sacrifício feito por eles em toda minha caminhada acadêmica. Por todo o apoio, os valores e o amor transmitido, serei eternamente grato.

Agredeço também aos meus irmãos, Gustavo Guimarães de Miranda e Gabriela Guimarães de Miranda, e suas famílias, pelos momentos de compreensão pela minha ausência, sempre enrolado e desesperado com os prazos da faculdade, e pelo apoio e amor que sempre me deram.

Agradeço à minha noiva, Maria Augusta Viegas, por acreditar em mim e me fazer ter coragem de enfrentar os obstáculos. Obrigado por dividir a vida comigo.

Agradeço ao professor Bruno Marx, por todas as vezes em que deu boas sugestões e por todo o material que compartilhou conosco.

Agradeço também à banca examinadora deste trabalho, professores Jorge Augusto e Juliana Sabino, por terem aceitado o convite e pela contribuições feitas no projeto e as que serão feitas aqui.

Agradeço ao professor e orientador, Vinicius Facó Ventura Vieira, pela dedicação, paciência, conhecimento e todo o esforço investido na construção desse trabalho.

Resumo

Atualmente, muito tem se discutido sobre a importância da criptografia na segurança dos dados utilizados a todo momento em um mundo cada vez mais informatizado. Com isso, se torna de suma importância discutir como se dá o processo de criptografia, com enfoque no método mais utilizado atualmente, RSA. Este trabalho tem a intenção de discutir e fundamentar esse método criptográfico e pormenorizar os passos que o compõe, como alternativa para o desenvolvimento do pensamento computacional. Primeiramente, será feita uma discussão sobre pensamento computacional e metodologias ativas e sobre o processo evolutivo da criptografia. Em um segundo momento, um aporte teórico acerca das bases matemáticas para o entendimento da criptografia RSA e, por último, a enunciação do método em si.

Palavras-chaves: Criptografia; RSA; Teoria dos Números.

Abstract

Lately, much has been discussed about the importance of encryption in the security of data used at all times in an increasingly computerized world. With this, it becomes extremely important to discuss how the encryption process takes place, focusing on the most used method nowadays, RSA. This work intends to discuss and substantiate this cryptographic method and to detail the steps that compose it, as an alternative for the development of computational thinking. First, we will discuss about computational thinking and active methodologies and about the evolutionary process of cryptography. In a second moment, a theoretical contribution about the mathematical bases for the understanding of RSA cryptography and, finally, the enunciation of the method itself.

Keywords: Cryptography; RSA; Number Theory.

Lista de ilustrações

Sumário

1 Introdução

Quase tudo o que se faz hoje na internet, desde o envio de uma mensagem num aplicativo até a transação em um banco, é protegido e guardado por um processo chamado de Criptografia. Entendida de modo resumido como a "arte" de esconder mensagens importantes, a criptografia é usada desde a Grécia antiga. Ganhou muita importância no império romano, com a Cifra de César, e foi peça fundamental para a expansão desse império, um dos maiores e mais influentes da história do homem. E foi graças a criptografia que Alan Turing, matemático do século XX, pôde, ao mesmo tempo em que criava uma máquina protótipo para o computador, ajudar na derrota da Alemanha nazista e encurtar a Segunda Guerra Mundial em quase dois anos.

Hoje, com a expansão de tecnologias como o computador e do estudo da divisibilidade dos números inteiros, essa "arte" tem uma aplicação fundamental no dia a dia de todo ser humano: nossas informações estão quase todas armazenadas em grandes bancos de dados de grandes empresas. Isso significa que boa parte de nossas vidas (lugares por onde andamos, mensagens que enviamos, compras que fizemos na internet, dentre outras coisas) estão criptografadas, salvas em forma de códigos/sequências numéricas, sob a posse de pessoas que nem sequer conhecemos. Pedro Adão, no livro "Números, cirurgias e nós de gravata", atesta essa ideia dizendo:

> Hoje em dia, complexos protocolos criptográficos protegem as nossas interações na internet, desde o simples acesso de serviços de e-mail ou redes sociais, até aplicações de homebanking ou transações entre grandes entidades financeiras. A criptografia é também extensivamente utilizada para garantir a integridade dos dados. Exemplos desta utilização são as assinaturas digitais em e-mails e registro de transações. (ADÃO, 2012, p.284)

Podemos ainda citar o fato de que o mercado financeiro mundial vem sofrendo algumas mudanças com a criação e propagação das criptomoedas, que são moedas digitais criptografadas. É possível que, em alguns anos, a humanidade não precise mais usar dinheiro em cédulas ou cartões, como nós conhecemos hoje, mas apenas como sequências de números criptografados. Assim como as mensagens pelo celular substituíram, em grande parte, o uso de cartas, as criptomoedas podem vir a substituir o dinheiro físico. Esses dois fatos já bastam para que fiquemos intrigados e curiosos sobre o assunto.

Além disso, o estudo da criptografia e seus desdobramentos pode ser justificado e fomentado pela necessidade, defendida bela Base Nacional Comum Curricular (BNCC) e por outros autores do meio educacional, de se desenvolver, nos alunos dos ensinos fun-

damental e médio, o pensamento computacional, como pode ser visto nesse trecho da própria BNCC:

> A área de Matemática, no Ensino Fundamental, centra-se na compreensão de conceitos e procedimentos em seus diferentes campos e no desenvolvimento do pensamento computacional, visando à resolução e formulação de problemas em contextos diversos. No Ensino Médio, na área de Matemática e suas Tecnologias, os estudantes devem consolidar os conhecimentos desenvolvidos na etapa anterior e agregar novos, ampliando o leque de recursos para resolver problemas mais complexos, que exijam maior reflexão e abstração. Também devem construir uma visão mais integrada da Matemática, da Matemática com outras áreas do conhecimento e da aplicação da Matemática à realidade. (BRASIL, 2018, p.470)

Segundo a BNCC, os alunos precisam desenvolver um pensamento computacional para facilitar a resolução de problemas complexos que exigem maior abstração matemática. Alem disso, espera-se que os alunos consigam usar o raciocínio computacional para aplicação da matemática na realidade. Neste sentido, acreditamos que o estudo dos métodos criptográficos, com enfoque no método RSA, pode contribuir para esse fim. Portanto, é cada vez mais importante que professores de matemática entendam como funciona a criptografia e quais as nuances desse processo.

Num primeiro momento, discorreremos sobre a definição e as discussões que envolvem o pensamento computacional e possíveis formas de trabalhá-lo. Para isso, falaremos sobre aprendizagem ativa, resolução de problemas e metodologias ativas de ensino. Daremos ainda ideias de atividades, baseadas em metodologias ativas, em que possam ser trabalhados conteúdos de criptografia a níveis básicos de ensino, enquanto se devenvolve o pensamento computacional.

Depois, focaremos na contextualização histórica da criptografia, até o método mais comum nos dias de hoje, o já citado método RSA. Neste processo, podemos observar a evolução metodológica do tema e perceber a importância da criptografia em diferentes contextos, como no caso da morte da rainha escocesa Mary Stuart, em 1587. Por conta de cartas suas que foram criptografadas, Mary Sturdat foi condenada a morte por sua prima, então rainha da inglaterra, Elizabeth I, com a justificativa de conspiração contra a coroa e traição. Esse episódio é conhecido como *A conspiração de Babington* - ver CIMINO(2018).

Posteriormente se observa, durante o estudo histórico da evolução da criptografia, que a matemática ganha notoriedade enquanto os processos criptográficos avançam, ou seja, a evolução da criptografia acompanha a evolução matemática. Portanto, se mostra importante falarmos dos métodos matemáticos que fundamentam os métodos de criptografia mais eficientes.

Fundamentaremos os conceitos básicos da Teoria dos números, tendo como ponto de partida o Principio da Boa Ordenação e o Princípio da Indução Finita. Falaremos sobre

propriedades dos números inteiros, com destaque para os números primos, até o teorema fundamental da aritmética. Depois, falaremos sobre aritmética modular, construindo a base para a enunciação do Teorema de Euler.

A evolução simultânea e paralela da criptografia e da matemática fez com que uma área alimentasse a outra: por um lado, o aperfeiçoamento dos métodos criptográficos trouxe desenvolvimento na matemática e, por outro, o desenvolvimento da matemática abriu novas possibilidades de métodos criptográficos mais eficientes.

Em posse de conhecimentos matemáticos mais específicos que fundamentam os métodos criptográficos mais utilizados hoje, podemos então introduzir com mais detalhes o método RSA. A escolha de se falar desse método se deu principalmente por dois motivos. O primeiro deles é a alta confiabilidade em sua segurança e o segundo advém do primeiro: esse método é o mais utilizado nos aplicativos e sites da internet.

Pensando nisso, entendemos que é importante que professores de matemática se capacitem no tema da Criptografia e possam ensinar para os alunos nas fases de ensino básico. Este trabalho, portanto, tem por objetivo discutir e fundamentar o método de criptografia RSA e pormenorizar os passos que o compõe, como alternativa para o desenvolvimento do pensamento computacional. Veremos seções envolvendo os temas propostos (pensamentos computacional e metodologias ativas, contextualização histórica, bases matemáticas e o próprio método RSA), voltados para professores em formação ou em formação continuada.

2 Pensamento computacional e a BNCC

Ao tentar definirmos o que é o pensamento computacional e como ele pode ser trabalhado, recorreremos à definição dada pelos autores do livro "Pensamento computacional". Segundo Santos et al. (2021, p.14), "o pensamento computacional pode ser definido como uma estratégia baseada no uso da tecnologia para projetar soluções e resolver problemas de forma eficaz"

Os autores Solange Fernandes, Luis Pereira, Roberta Fleira e Douglas Dantas, em seu livro "Novas trajetórias de formação - Matemática" explicam como essa resolução de problemas se dá exatamente, quando dizem:

> O pensamento computacional prevê a decomposição de um problema complexo em problemas mais simples, em uma técnica conhecida como "dividir para conquistar". O objetivo dessa técnica é permitir a abordagem pontual e focada em cada parte do problema. Uma vez resolvidos de forma autossuficiente, os problemas menores são reunidos e a solução completa pode ser implementada.(FERNANDES et al., 2021, p.96)

Neste sentido, uma forma possível de se trabalhar o pensamento computacional é utilizando uma abordagem pedagógica conhecida como *Resolução de problemas*.

2.1 Resolução de problemas

Essa metodologia de ensino, como o nome sugere, se baseia na resolução de problemas para o aprendizado, dando enfoque em todo o processo dessa resolução e não somente no produto final.

Para ECHEVERIA e POZO (1988), "a solução do problema exige uma compreensão da tarefa, a concepção de um plano que nos conduza à meta, a execução desse plano e, finalmente, uma análise que nos leve a determinar se alcançamos ou não a meta.". Ou seja, existem alguns passos que definem e fundamentam a resolução de problemas. Ao mesmo tempo, esses mesmos passos também fundamentam o desenvolvimento do pensamento computacional.

Continuando a leitura do livro "Novas trajetórias de formação - Matemática", os autores detalham com mais precisão o que chamaram de "dividir para conquistar", detalhando algumas capacidades importantes contempladas ao se trabalhar o pensamento computacional para resolução de problemas:

> A primeira delas é a de compreender. Pode parecer simples, mas a correta interpretação de um problema, suas características, parâmetros,

> restrições, atores envolvidos e objetivos é uma tarefa complexa. Pode haver barreiras de linguagem, pressão por tempo escasso, falta de conhecimento do assunto, entre outras. Uma abordagem mal conduzida, incompleta ou errônea certamente leva a uma solução que não resolve o problema em questao.(FERNANDES et al., 2021, p.97)

De fato, só se faz possível encontrar uma solução para determinado problema se primeiro o entendemos. Ou seja, se quem está tentando resolvê-lo compreende aquilo que o problema exige.

Para além da interpretação, porém, existe a habilidade de saber analisar o problema. Depois de se interpretar o que se pede, se faz necessário entender os passos que devem ser tomados a fim de revolvê-lo. Se num problema de progressão aritmética, por exemplo, um aluno interpreta erroneamente o caso e calcula um termo dessa progressão utilizando a fórmula geral do termo de uma progressão geométrica, certamente o resultado encontrado não será o que se espera. Essa segunda capacidade é explicitada no trecho:

> A segunda capacidade importante é a de analisar. Esse item está ligado ao aprofundamento do conhecimento necessário para conduzir a elaboração dos procedimentos de solução. Entender todo o escopo, verificar ferramentas e recursos disponíveis e a viabilidade de utilização fazem parte dessa capacidade.(FERNANDES et al., 2021, p.97)

Como terceiro passo, temos o mais dificil dentre os três:

> Uma vez entendido e analisado o problema, inicia-se a fase da modelagem, a fim de aplicar uma solução a um caso menor, restrito e mais controlado, para conferir a eficácia do mecanismo em desenvolvimento. Modelado o problema, busca-se a definição de padrões e, a partir deles, entra-se na busca pela generalização. Ela permitirá que problemas maiores possam ser resolvidos com o mesmo algoritmo, que, uma vez definido e otimizado, serve como uma receita a ser seguida (FERNANDES et al., 2021, p.97)

Modelar um problema menor, com o intuito de tentar encontrar padrões que possam ser replicados em problemas maiores, pode ser uma tarefa difícil. Não são todas as pessoas que possuem alguma facilidade em matemática que conseguem generalizar a resolução de um problema específico, de forma a criar um algoritmo que valha para todos os casos. Esse é um trabalho que fica a cargo dos cientistas e acadêmicos matemáticos.

Vale notar que os passos supracitados têm coerência, e são na verdade os mesmos propostos por George Polya, em seu livro *Arte de resolver problemas*. Neste livro, polya nos diz que são necessários quatro passos a fim de se resolver um problema, sendo eles:

> Primeiro, temos de compreender o problema, temos de perceber claramente o que é necessário. Segundo, temos de ver como os diversos itens estão inter-relacionados, como a incógnita está ligada aos dados, para

> termos a ideia da resolução, para estabelecermos um plano. Terceiro, executamos nosso plano. Quarto, fazemos um retrospecto da resolução completa, revendo-a e discutindo-a. (POLYA, 1995, p.3)

A *Resolução de problemas*, portanto, é uma ferramenta educacional que permite o desenvolvimento do pensamento computacional, uma vez que engloba os passos necessários que o fundamentam. E, por outro lado, o desenvolvimento do pensamento computacional facilita a aplicação da *Resolução de problemas*, pelo mesmo motivo.

Apesar de não trazer, em seu texto, essa ligação existente entre pensamento computacional e resolução de problemas, a BNCC discorre sobre o tema, de forma a incentivar que os professores de matemática se preocupem com o desenvolvimento do pensamento computacional de seus alunos.

2.2 Pensamento computacional na BNCC

O pensamento computacional é uma ferramenta importante para que cada aluno tenha à sua disposição na hora de lidar com problemas - sejam questões de provas e vestibulares, sejam problemas da vida cotidiana de cada um. E para que se desenvolva esse tipo de raciocínio no aluno, a BNCC nos diz que é também necessário que seja feito um bom trabalho com as disciplinas comuns previstas para o ensino de Matemática nos ensinos fundamental e médio, já que dividir problemas maiores em partes menores é uma estratégia importante em disciplinas de matemática. (BRASIL, 2018).

Além disso, para o desenvolvimento do pensamento computacional, a BNCC ainda propõe que sejam estudados algorítmos e fluxogramas, como pode ser visto no trecho abaixo:

> Associado ao pensamento computacional, cumpre salientar a importância dos algoritmos e de seus fluxogramas, que podem ser objetos de estudo nas aulas de Matemática. Um algoritmo é uma sequência finita de procedimentos que permite resolver um determinado problema. Assim, o algoritmo é a decomposição de um procedimento complexo em suas partes mais simples, relacionando-as e ordenando-as, e pode ser representado graficamente por um fluxograma. A linguagem algorítmica tem pontos em comum com a linguagem algébrica, sobretudo em relação ao conceito de variável. Outra habilidade relativa à álgebra que mantém estreita relação com o pensamento computacional é a identificação de padrões para se estabelecer generalizações, propriedades e algoritmos.(BRASIL, 2018, p.267)

Algoritmos e fluxogramas são ferramentas que ajudam a formar a base de quase todo o conhecimento que envolve a computação. São, portanto, uma área de interseção entre o pensamento computacional e o estudo do método de criptografia RSA, dado que esse método se baseia na aplicação de um algoritmo (uma sequência de passos a ser seguida) tanto para codificar, quanto para decodificar as mensagens.

Vale salientar ainda que essa não é a única interseção entre o desenvolvimento do pensamento computacional e o estudo de criptografia. Para a BNCC "[...] destaca-se ainda a importância do recurso a tecnologias digitais e aplicativos tanto para a investigação matemática como para dar continuidade ao desenvolvimento do pensamento computacional, iniciado na etapa anterior."(BRASIL, 2018). Neste ponto, então, há outra convergência entre pensamento computacional e criptografia, já que o uso de tecnologias é muito comum quando se trata de criptografia nos dias atuais. São necessários computadores de alta performance para que todo o processo de criptografia do método RSA se desenvolva.

Portanto, o estudo do método RSA se faz útil também no sentido de ajudar no desenvolvimento do pensamento computacional, uma vez que esse método criptográfico usa noções e conceitos matemáticos, além de fluxogramas e algorítimos - esse estudo pode ser desenvolvido por meio de metodologias ativas.

Mas o que são e por que as metodologias ativas ajudariam nesse processo? As metodologias ativas são um conjunto de abordagens educacionais cujo objetivo é fazer do aluno o personagem principal do processo de ensino-aprendizagem, ou seja, que os alunos absorvam os conteúdos de forma autônoma e participativa. Diferentemente do ensino tradicional, nas metodologias ativas o que importa é o processo da construção do conhecimento e não somente o produto final - e aqui se encontra a principal vantagem de se usar esse método de ensino: entender o caminho traçado para se chegar a um determinado conhecimento permite ao aluno entender de fato o conteúdo e não somente "gravá-lo" para a resolução de uma prova, por exemplo. Em seu livro "*Metodologias Inovativas na educação presencial, a distância e corporativa*", as autoras Andrea Filatro e Carolina Costa Cavalcanti trazem uma definição das metodologias ativas que reforçam aquilo que queremos:

> As metodologias ativas são estratégias, técnicas, abordagens e perspectivas de aprendizagem individual e colaborativa que envolvem e engajam os estudantes no desenvolvimento de projetos e/ou atividades práticas. Nos contextos em que são adotadas, o aprendiz é visto como um sujeito ativo, que deve participar de forma intensa de seu processo de aprendizagem (mediado ou não por tecnologias), enquanto reflete sobre aquilo que está fazendo.(FILATRO, 2018, p.12)

2.3 Metodologias ativas e criptografia

Apesar do método RSA e Criptografia em geral envolverem uma boa base matemática na Teoria dos números, usando algumas metodologias ativas que aumentem o interesse dos alunos, acreditamos que seja possível ensinar esse tema para níveis mais básicos de ensino - mais à frente, são dadas algumas sugestões de como isso pode ser feito. A BNCC nos dá um parâmetro de como deve ser a educação matemática no ensino fundamental:

> Da mesma forma que na fase anterior, a aprendizagem em Matemática no Ensino Fundamental - Anos Finais também está intrinsecamente relacionada à apreensão de significados dos objetos matemáticos. Esses significados resultam das conexões que os alunos estabelecem entre os objetos e seu cotidiano, entre eles e os diferentes temas matemáticos e, por fim, entre eles e os demais componentes curriculares. Nessa fase, precisa ser destacada a importância da comunicação em linguagem matemática com o uso da linguagem simbólica, da representação e da argumentação.(BRASIL, 2018, p.276)

Tendo como referência o texto da BNCC, a proposta aqui é escolher alguns métodos já conhecidos e pô-los em prática no ensino da criptografia.

Entendemos que esse conteúdo deve ser trabalhado de forma que os alunos sejam ativos em todo o processo, na tentativa de evitar que se torne um peso, ao invés de agregar conhecimento. Para isso, recomendamos que as aulas tenham como base a metodologia de ensino conhecida como *aprendizagem ativa*. Essa metodologia consiste em colocar o aluno como centro de todo o processo de ensino-aprendizagem e possui algumas vantagens, como destaca um dos os autores do livro "Metodologias para aprendizagem ativa":

> As metodologias ativas, além de representarem uma alternativa pedagógica capaz de proporcionar ao aluno a capacidade de transitar de forma mais autônoma dentro de seu próprio percurso de aprendizagem, pode ser um caminho para que ele desenvolva habilidades úteis para seu futuro, sabendo gerar respostas para problemas e conflitos dos campos profissional e social.(BES et al., 2019, p.19)

Luckesi corrobora com essa metodologia quando diz:

> A aprendizagem ativa é aquela construída pelo educando a partir da assimilação ativa dos conteúdos socioculturais. Isso significa que o educando assimila esses conteúdos, tornando-os seus, por meio da atividade de internalização de experiências vividas.(LUCKESI, 2002, p.132)

Portanto, o que pretendemos aqui é que os alunos aproveitem a jornada no entendimento da criptografia, com enfoque no método RSA. Que eles tentem entender o mundo a sua volta, cada vez mais dependente de processos criptográficos, de forma criativa e prática. Ou seja, que os professores não se limitem a passar apenas o conteúdo teórico e que pensem além de uma aula com somente quadro e caneta. D' Ambrosio nos mostra a dinâmica da sala de aula tradicional, dizendo:

> Sabe-se que a típica aula de matemática a nível de primeiro, segundo ou terceiro graus ainda é uma aula expositiva, em que o professor passa para o quadro negro aquilo que ele julgar importante. O aluno, por sua vez, copia da lousa para o seu caderno e em seguida procura fazer exercícios de aplicação, que nada mais são do que uma repetição na aplicação de um modelo de solução apresentado pelo professor. (D'AMBROSIO, 1989, p.15)

A fim de comparar a aprendizagem ativa com o método de ensino tradicional, Libâneo defende que o papel do professor deve ser o de mediador de todo o processo de ensino aprendizagem, o que permite o desenvolvimento de habilidades e competências dos alunos, que provavelmente ficariam atrofiadas no método de ensino tradicional:

> O ensino exclusivamente verbalista, a mera transmissão de informações, a aprendizagem entendida somente como acumulação de conhecimentos, não subsistem mais. Isso não quer dizer abandono dos conhecimentos sistematizados da disciplina nem da exposição de um assunto, o que se afirma é que o professor medeia a relação ativa do aluno com a matéria, inclusive com os conteúdos próprios de sua disciplina, mas considerando os conhecimentos, a experiência e os significados que os alunos trazem à sala de aula (...) Ao mesmo tempo, o professor ajuda no questionamento dessas experiências e significados, provê condições e meios cognitivos para sua modificação por parte dos alunos e orienta-os, intencionalmente, para objetivos educativos. Está embutida aí a ajuda do professor para o desenvolvimento das competências do pensar, em função do que coloca problemas, pergunta, dialoga, ouve os alunos, ensina-os a argumentar, abre espaço para expressarem seus pensamentos, sentimentos, desejos, de modo que tragam para a aula sua realidade vivida. É nisso que consiste a ajuda pedagógica ou mediação pedagógica.(LIBÂNEO, 1998, p.13)

Assim, para que esse estudo faça do aluno um protagonista de fato, usaremos algumas das metodologias ativas mais conhecidas.

O ensino de criptografia pautado em metodologias ativas será mais frutuoso e, portanto, corresponderá à importância que esse tema tem em nossas vidas nos dias de hoje, além de deixar mais leve um tema que pode ser maçante, uma vez que contém uma base teórica de matemática razoavelmente extensa, se passado de forma monótona.

Das metodologias ativas mais conhecidas e utilizadas, podemos citar: Sala de aula invertida que, como o próprio nome sugere, propõe a inversão dos papéis na sala de aula: os alunos ficam com o dever de se prepararem previamente e ensinar seus colegas, enquanto o professor age como um aluno, de forma mais pacífica e pronto para dar sugestões, se achar necessário. Segundo os autores do livro "Revolucionando a sala de aula 2 - Novas metodologias ainda mais ativas", a dinâmica da sala de aula invertida se dá da seguinte maneira:

> Os conceitos são passados aos alunos antes do início da aula, por meio do uso de alguma tecnologia de informação e comunicação (TIC), e o tempo em sala de aula é usado para dúvidas, discussões, atividades em grupo ou individual, dinâmicas, laboratório, entre outros recursos. A ideia é aproveitar a presença do professor para aquelas atividades nas quais sua presença é decisiva (NOGUEIRA et al., 2020, p.77)

Podemos também destacar a Gamificação, que é um método que pretende usar ferramentas e jogos para fins didáticos, podendo variar de jogos de tabuleiros, por exemplo, até softwares de computadores. Outra metodologia, muito usada nas aulas de matemática

é a modelagem matemática, que simplifica problemas da vida cotidiana ao modelá-los matematicamente, o que traz a aula para mais perto da vida pessoal dos alunos e que, por sua vez, desperta seus interesses. Além de outros métodos, como rotação por estações de aprendizagem, aprendizagem baseada em problemas e ensino híbrido.

2.3.1 Ideias de atividades para o ensino de criptografia

Veremos, agora, algumas formas em que o conteúdo a ser trabalhado nesta monogradia pode ser aplicado na sala de aula. Vale notar que, como não é o foco de nosso trabalho, aqui serão dadas breves noções de como essa aplicação poderia ser feita.

Para o estudo da criptografia, podemos começar usando Storytelling, uma metodologia ativa que busca criar narrativas para explicar o conteúdo a ser trabalhado. A contação de histórias é uma prática muito antiga, desde os primórdios do homem neste mundo, que tem sua força até hoje. Segundo MAX (2015, p.9) "Os estudiosos, antropólogos e historiadores, atestam que gostar de contar e escutar narrativas é um comportamento ancestral da humanidade". Na página seguinte, complementa: MAX (2015, p.10) "Apreciar histórias é dos aspectos mais comuns, antigos e profundos da alma humana. Todo homem, a priori, gosta de contar e de ouvir boas histórias."

Contando uma história com elementos que prendam a atenção, pode-se passar a parte histórica da criptografia como um todo, parte essa que envolve guerras, impérios, reis e segredos obscuros.

Como sugestão, pode-se passar como um trabalho que os alunos montem uma peça de teatro em que um deles será um mensageiro romano, alguns outros serão soldados de uma nação inimiga, como um grupo de nórdicos da região de Gália e outro aluno será o imperador romano Júlio César. O enredo consistirá em: os inimigos romanos interceptaram o mensageiro, que levava consigo uma importante mensagem do imperador para um destacamento de centuriões em determinada região e agora estão tentando decifrar o que está escrito ali.

Depois, para ver o conteúdo matemático de forma mais lúdica, pode-se usar a já citada Gamificação. Do já citado livro "Revolucionando a sala de aula 2", podemos ver essa definição de Gamificação:

> O emprego de jogos, atividades de jogos ou elementos de jogos, por exemplo medalhas, rankings, recompensas etc., para motivar e envolver estudantes no processo de educação, com o intuito de elevar a aprendizagem. A Gamificação não compreende, obrigatoriamente, o uso de jogos verdadeiros ou de tecnologias da informação e comunicação. Todavia, a incorporação de elementos, padrões ou circunstâncias que são usualmente encontrados em jogos aos processos de aprendizagem com o intuito de encorajar comportamentos desejados nos alunos pode ser considerada a Gamificação da educação (NOGUEIRA et al., 2020, p.129)

Nesse sentido, podemos pensar em algumas sugestões de como aplicá-la em sala de aula:

1. Propor jogos que trabalhem com o resto da divisão de números inteiros para se iniciar o estudo da congruência: pedir para que os alunos, em duplas, passem contas uns para os outros, com perguntas do tipo "quanto é a divisão de 40 por 3?", contabilizando pontos para ver quem vence ao final, por exemplo. Esse tipo de atividade serviria para se trabalhar conceitos matemáticos que servem como base para a criptografia.

2. Ou ainda, passar os métodos mais embrionários de criptografia, como a já citada Criptografia de César, na forma de um jogo: Escrever, no quadro, alguma mensagem embaralhada com essa cifra e estipular um tempo para que os alunos, divididos em grupos, façam uma criptoanálise e tentem descobrir a chave e a mensagem original. O grupo que primeiro descobrir, ganha alguma gratificação.

Também cabe como sugestão usar a Modelagem matemática para trazer à sala de aula problemas reais enfrentados por criptoanalistas e criptógrafos ao longo dos anos (isso poderia inclusive ser feito juntamente com o Storytelling), até chegar nos problemas atuais envolvendo os números primos e a criptografia RSA.

Como sugestão, pode-se dividir a turma em grupos, como se fossem grupos de criptoanalistas imitando o grupo de Alan Turing durante a Segunda Guerra Mundial, e pedir que tentem, a partir de algumas mensagens criadas, descobrir algum padrão que possa ser utilizado para quebrar a Enigma. Nesse caso, não cabe pedir que os alunos façam um trabalho como o de Turing e sua equipe (construção de um computador para decifrar uma máquina muito inteligente), mas vale estimular neles que consigam chegar os primeiros passos que Turing chegou.

Por último, podemos utilizar a investigação matemática. Segundo Ponte, Brocardo e Oliveira (2007, p.13) "Para os matemáticos profissionais, investigar é descobrir relações entre objetos matemáticos conhecidos ou desconhecidos, procurando identificar as respectivas propriedades"

Portanto, abre-se um leque grande, ao se pensar na base matemática do método de criptografia RSA, para usar essa metodologia ativa. Alguns dos resultados sobre os números inteiros, trabalhados mais à frente neste trabalho, têm uma demonstração relativamente tranquila e podem ser passadas como uma atividade de investigação matemática.

3 História da criptografia

A proteção de nossos dados feita pela criptografia tem muita importância devido ao fato de guardar nossa privacidade. Não seria nada agradável se qualquer pessoa pudesse ter acesso às conversas, mensagens e outras mídias enviadas de nossos dispositivos. Porém, essa necessidade de guardar informações não é nova. Segundo Cimino (2018, p.1), no decorrer da história do homem, sempre houve a necessidade de sigilo. Ainda no mesmo livro, o autor pontua que:

> No mundo antigo, a arte da escrita secreta era cultivada do mesmo modo como determinadas profissões desenvolvem um jargão próprio e gangues usam gírias - como insígnia de identificação e para excluir os de fora. Mas, quando a guerra ficou mais sofisticada, os códigos e cifras se tornaram uma arma essencial para transmitir estratégias e outras informações vitais sem entregar o ouro ao inimigo. (CIMINO, 2018, p.11)

Em outras palavras, existem registros antigos de linguagem criptográfica, como no caso da tumba de Khnumhotep II, do Egito, que não serviam para esconder alguma mensagem, mas apenas para que o escriba pudesse demonstrar suas habilidades artísticas. Porém, quando as cifras passaram a ser usadas como máquinas de guerra, seja na guerra declarada, a fim de guardar e transmitir estratégias e informações importantes, seja na guerra silenciosa que se dá no trabalho dos espiões, foi que os verdadeiros avanços nessa área surgiram e a criptografia ganhou o status de ciência.

Ao longo dos anos, foram travadas muitas disputas entre codificadores e decifradores de códigos, o que permitiu um avanço nas descobertas científicas acerca do assunto. Ao passo que os decifradores iam trazendo à luz as lacunas e fragilidades dos métodos criptográficos usados em cada época, os codificadores eram impelidos a criarem métodos mais fortes - métodos que tornassem a mensagem o mais difícil possível de ser decifrada.

Para começarmos, então, nosso breve passeio pela história da criptografia, começaremos falando sobre uma técnica de codificação muito usada na antiguidade: a cifra de transposição.

3.1 Crifra de Transposição

Esse modo de cifrar uma mensagem é na verdade muito simples. Consiste em embaralhar as letras da mensagem original de alguma forma previamente combinada entre o remetente e o destinatário. O deslocamento das letras faz com que se crie anagramas que não dizem nada para aqueles que não conhecem a chave de criptografia. Como exemplo, invertendo cada trio de letras, ignorando os espaços entre elas, podemos transformar a

mensagem “Leve dez besteiros para a torre” em “Veledeebzetsoriapsaarroter”. Para voltar à mensagem original, basta fazer o processo inverso.

Apesar de a mensagem cifrada nesse exemplo ser aparentemente dificil de ser entendida, veremos, com um outro exemplo, como a cifra de transposição pode ser na verdade simples de ser quebrada. Agora, nossa chave de codificação será: em todas as palavras, fixaremos a primeira sílaba e inverteremos as letras das outras sílabas, além de ignorarmos as vírgulas. Assim, a mensagem “Temos duzentos homens, entre cavaleiros e arqueiros, esperando na retaguarda” seria codificada como “Tesom dunezsot hosnem denert caavielsor e arieuqsor esespnarod an reatraugad”. As palavras de nossa mensagem cifrada, neste caso, não se distinguem tanto das palavras originais, além do fato de que a conjunção “e” não tem como ser mudada e a palavra “na” é fácil de ser decodificada, já que possui apenas duas letras.

A técnica de criptografia por transposição foi amplamente utilizada no império romano, com o suporte de um instrumento chamado cítala ou bastão de Licurgo. Segundo Cimino (2018, p.17), “uma tira estreita de couro ou pergaminho era enrolada num bastão; depois, a mensagem era escrita na etensão do bastão, com uma letra em cada volta da tira. Quando desenrolada, a tira mostrava uma longa coluna de letras misturadas”. Para decifrar a mensagem, o destinatário precisava estar em posse de um bastão de espessura muito próxima do primeiro e então enrolar a tira de couro nele para ver a sequência certa das letras.

Figura 1 – Cítala romana.

Fonte: Wikipédia, 2007

Além da técnica de cifra de transposição, outra que foi muito utilizada é a cifra de substituição que, como veremos, pode ser expressa em exemplos simples do mundo antigo, mas que graças à evolução desse tipo de cifra, a criptografia pôde galgar passos maiores, que nos levaram aos métodos criptográficos usados hoje.

3.2 Cifra de Substituição

A cifra de substituição, como o nome sugere, se baseia em substituir as letras ou palavras da mensagem original por outras letras ou palavras combinadas entre as partes interessadas na mensagem.

3.2.1 Cifra de César

Dos métodos de cifra de substituição, talvez o mais conhecido seja a Cifra de César. O imperador romano Júlio César se comunicava com seus generais por mensagem cifradas de uma forma bem simples: cada letra do alfabeto era substituída por uma letra que ficava 3 posições à frente desta, por exemplo. Neste caso, a letra “a” se torna “d”, a letra “g” se torna “j” e assim por diante. Poderíamos, então, codificar a mensagem "Centuriões"em “Fhqwxulrhv”. Para decifrar, basta pegar cada letra da mensagem cifrada e voltar três letras - para isso, é claro, tanto quem envia quanto quem recebe a mensagem devem conhecer a chave (nesse caso, a chave seria “3 posições”). Esse tipo de chave recebe o nome de chave simétrica, pois se usa uma mesma chave para cifrar e decifrar o código.

Ainda que alguém não conheça a chave de codificação, o método não se torna forte. As mensagens codificadas com a Cifra de César são fáceis de serem descobertas por alguém indesejado - basta que a pessoa que pegou a mensagem cifrada teste todas as opções de letras possíveis.

Aqui vale ressaltar que a ideia de testar todas as opções de letras possíveis no alfabeto, conhecida como criptoanálise sistemática, surgiu alguns séculos depois, com o polímata árabe Abu al-Kindî. No século IX, Abu al-Kindî escreveu um manuscrito chamado “Da elucidação de correspondência codificada”, em que explicava como decodificar um documento usando análise de frequência. Essa forma de decodificação pode ser explicada, resumidamente, da seguinte maneira: em cada alfabeto, existem letras que aparecem com maior frequência que outras e, portanto, conhecendo-se a língua em que foi escrita a mensagem codificada, podemos substituir a letra que mais aparece na mensagem pela letra que mais aparece no alfabeto desta língua e assim seguir usando as outras letras e suas frequências. No caso da língua portuguesa, por exemplo, poderíamos trocar a letra que mais aparece na mensagem cifrada pela letra “a”, já que esta é a letra com maior frequência nas palavras em português. Depois, trocaríamos a segunda letra que mais aparece na mensagem cifrada pela letra “o”, que é a segunda letra com maior frequência em nossa língua. Seguiríamos esse processo até que tivéssemos decodificado toda a mensagem.

Faremos um segundo exemplo, dessa vez com uma mensagem um pouco maior, a fim de verificarmos a fraqueza desse método a partir da análise de frequência. Ainda usando a mesma chave de codificação do primeiro exemplo, codificamos a mensagem "Atacaremos a Pérsia pelo flanco esquerdo” em “Ewefeuhprv e shuvle shor ioeqfr hvtzhugr”.

Usando a análise de frequência, trocaríamos cada "e" de nossa mensagem cifrada pela letra que mais aparece no alfabeto português, "a", e nesse caso já teríamos uma boa parte da mensagem decodificada. Poderíamos ainda nos atentar ao fato de que existe um "e", em nossa mensagem codificada, que está sozinho e que, portanto, conhecendo a língua em que a mensagem foi escrita, sabemos que essa letra se trata de um artigo definido, já que não poderia ser a conjunção aditiva "e" - se fosse, a mensagem, na verdade, não estaria codificada. Ou seja, só pode ser a letra "a" ou a letra "o" na mensagem original.

As cifras de substituição monoalfabéticas (chamadas assim por utilizarem somente um alfabeto para a codificação), como a de César, foram muito confiáveis por muito tempo. Quando, porém, as fraquezas dessas cifras ficaram evidentes, como no caso da Conspiração de Babington, citada na introdução, se fez necessário incrementar os métodos criptográficos existentes. É diante desse cenário que o arquiteto e estudioso italiano Leon Battista Alberti apresenta uma invenção interessante.

3.2.2 Cifras de Substituição polialfabéticas

Segundo Carneiro (2017, p.8), "Leon Alberti propõe usar dois ou mais alfabetos e alterná-los durante uma cifragem de modo a evitar a análise de frequência das letras do idioma". Esse processo ficou conhecido como disco de Alberti.

Essa ferramenta era construída da seguinte forma: dois círculos de cobre, com uma pequena diferença em seus diâmetros, eram sobrepostos e tinham um alfabeto escrito ao longo de suas bordas. Colocava-se então uma agulha, passando pelos centros dos círculos, que servia como um eixo comum entre eles, permitindo que girassem de forma independente. Com os dois círculos girando, os dois alfabetos mudavam suas posições relativas, permitindo que se cifrasse a mensagem. O alfabeto do círculo maior, de fora, era tomado como o original, enquanto o do círculo menor, de dentro, era o cifrado. Cada letra da mensagem original era substituída pela letra correspondente no círculo menor.

Figura 2 – Disco de Alberti.

Fonte: Webdehistoria, 2014

A substituição polialfabética continuou se desenvolvendo aos poucos, até que o

diplomata francês Blaise de Vigenère, tomando como base o trabalho de Alberti, decidiu cifrar mensagens utilizando 26 alfabetos distribuídos em uma tabela, conhecida como Tabela de Vigenère. O sistema criado por ele foi chamado de "A cifra indecifrável"e funciona da seguinte maneira: estando em posse da tabela com os 26 alfabetos (ver abaixo), escolhe-se uma palavra para ser a chave, chamada de palavra-chave. Depois, escreve-se a palavra-chave sobre a mensagem original até que cada letra da mensagem corresponda a uma letra da palavra-chave. Assim, cada letra da mensagem original será trocada pela letra que é a interseção entre a letra da mensagem original (coluna) e a letra da palavra-chave (linha).

Figura 3 – Cifra de Vigenère.

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

Fonte: Wikipedia, 2011

Para que fique mais claro, façamos um exemplo: nossa mensagem a ser cifrada será "Ataque o norte" e a palavra-chave será "Verde". Assim, ao escrever a palavra-chave sobre a mensagem original, teríamos "verdev e rdeve". Nossa mensagem cifrada seria então "Vxrtyz s ervoi".

Note que a análise de frequência não é tão efetiva aqui, pois uma mesma letra é cifrada em letras diferentes. No nosso exemplo, a letra "a" foi substituída pelas letras "v" e "r" enquanto a letra "o" foi substituída por "s" e "r". Interessante ressaltar também que as duas letras foram cifradas em uma mesma letra, "r", o que dificulta ainda mais a vida dos criptoanalistas.

No entanto, ainda assim, na primeira metade dos anos 1800, dois homens foram capazes de quebrar a Cifra de Vigenère. Charles Babbage e Friedrich Wilhelm Kasiski, sendo o primeiro inglês e o segundo prussiano, conseguiram, de forma independente, notar que, na Cifra de Vigenère, sequências de letras se repetem frequentemente e que a cifra de substituição polialfabética da tabela de Vigenère é composta por várias cifras monoalfabéticas e que cada uma delas pode ser decifrada com a análise de frequência (apesar do trabalho mecânico necessário para isso).

3.3 Mecanização da criptografia

Com a quebra da Cifra de Vigenère, não houve grandes avanços na área da criptografia até o final da segunda metade do século XIX e, portanto, não haviam mais métodos confiáveis de criptografia. Até que, no ano de 1896, o matemático italiano Guglielmo Marconi, no auge de sua criatividade científica, inventou um dispositivo que mudou a história do mundo, conhecido como rádio: um aparelho que emitia e recebia pulsos elétricos há um distância de muitos quilômetros, sem a necessidade de fios condutores, como acontecia no caso dos telégrafos da época.

Essa invenção encantou muitas pessoas e, de modo especial, encantou os militares. Usar o rádio para se comunicar em uma guerra parecia uma ideia promissora, pela facilidade e velocidade de comunicação. Porém, havia um grande problema: as ondas de rádio podiam ser captadas por aparelhos indesejados e, portanto, os comandos de guerra se tornavam perigosos, pois poderiam cair nas mãos erradas a qualquer momento.

Diante dessa fragilidade exposta do rádio, muito tempo e recurso foi investido a fim de que fosse criado um novo método criptográfico que o tornasse seguro. Durante a primeira guerra mundial, porém, nada se criou de relevante e as comunicações nas guerras ainda eram feitas pelo dispositivo de Guglielmo Marconi.

Foi então na grande guerra seguinte, a Segunda Guerra Mundial, que surgiu uma invenção alemã que aparentemente não tinha fraqueza alguma, chamada de Enigma.

Enigma foi o nome dado à máquina criptográfica criada pelo engenheiro elétrico alemão Arthur Scherbius, máquina essa que foi usada pelos alemães para se comunicarem de forma segura durante a Segunda Guerra Mundial. Era composta de alguns rotores, um painel com letras e teclas parecidas com uma máquina de escrever.

De forma simplificada, a cada tecla que se digitava, piscava uma luz no painel indicando a letra codificada e os rotores giravam e mudavam a correspondência das letras da mensagem original com a codificação. Além disso, os operadores das máquinas Enigma recebiam um livreto contendo as instruções de como deveriam posicionar seus rotores todos os dias, a fim de que todos ficassem em sintonia na hora de criptografar e decifrar suas mensagens.

A Enigma parecia indecifrável pelo fato de que, se os alemães usassem sete rotores em suas máquinas, o número total de possibilidades de chaves era, segundo o próprio Arthur Scherbius, de seis bilhões. A Enigma podia comportar até 13 rotores. Em posse dela, os alemães parecem imparáveis. Mesmo quando os aliados conseguiam interceptar suas mensagens, não sabiam como decifrá-las.

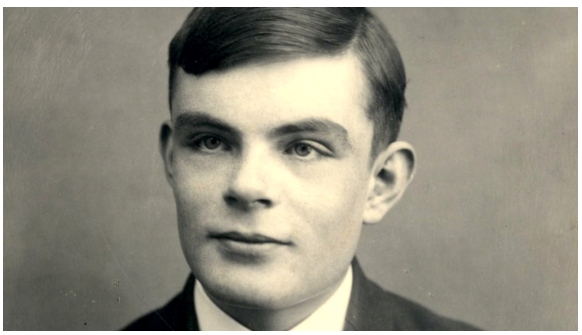
Diante desse colosso inventivo alemão, muitos foram os matemáticos da época que se dedicaram a decifrá-la, mas um deles se destacou como peça fundamental.

Figura 4 – Enigma.

Fonte: Wikipedia, 2011

Alan Turing, matemático inglês nascido em 1912, foi convidado pela Escola de Cifras e Códigos do Governo da Inglaterra, no ano de 1939, para tornar-se um dos criptoanalistas de uma equipe formada com o intuito de decifrar a Enigma. A busca pela quebra da cifra dos alemães durou ainda alguns anos, até que por volta do ano de 1945, Turing toma a iniciativa de seguir os caminhos do matemático polonês Marian Rejewski, que tinha quebrado uma versão mais antiga e arcaica do código de uma máquina precursora da Enigma (ver CIMINO), e junto com sua equipe de apoio, conseguiu decifrar as complicações adicionadas da Enigma. Isso possivelmente alterou o curso da guerra, que em vez de ter terminado em 1948, terminou 1945 (CARNEIRO, 2017). Além desse feito, a máquina criada por Alan Turing, chamada de máquina universal de Turing, serviu de base para os primeiros computadores, cerca de dez anos depois, segundo o que diz o autor Framilson José Ferreira Carneiro, em seu livro Criptografia e Teoria dos Números.

Figura 5 – Alan Turing.



Fonte: UOL, 2020

Para conseguir decifrar a Enigma, Turing e sua equipe observaram que todas as mensagens do exército alemão começavam sempre com a palavra “clima” e terminavam com a saudação nazista “Heil Hitler”. Assim, conseguiam, todos os dias, saber como os rotores das máquinas estavam dispostos e, usando sua cópia da Enigma, conseguiam

decifrar as mensagens alemãs.

Depois do feito de Turing, os matemáticos foram aperfeiçoando o computador até que, em meados de 1960, essas máquinas passaram a ser mais baratas e potentes. Grandes empresas, como bancos e supermercados, se interessaram pelo computador, que antes era usado exclusivamente pelos militares. Para poder armazenar de forma segura os dados bancários e suas transações, porém, era necessário um sistema de segurança confiável, ou seja, um método criptográfico dificil de ser decifrado.

Na busca de tentar padronizar os sistemas de criptografia usados por essas empresas e aumentar o número de chaves possíveis, dois cientistas da computação e um matemático, Ron Rivest, Adi Shamir e Leonard Adleman criaram um método de criptografia altamente seguro e largamente usado até os dias de hoje, conhecido como RSA - sigla que advém das iniciais dos sobrenomes de seus autores. Esse método é galgado na matemática e sua alta segurança é devida à congruência modular e os números primos.

No capítulo 6 falaremos em detalhes como funciona o método RSA e o porquê de ser altamente seguro. Antes disso, porém, é necessário relembrarmos alguns conceitos matemáticos que servem como base para o funcionamento do método.

4 Introdução a Teoria dos Números

Neste capítulo, relembraremos os conceitos básicos sobre Teoria dos Números para que possamos entender como funciona o método RSA. Começaremos com o Principio da Boa Ordenação, que pode ser posto como:

4.1 Princípio da Boa Ordenação (PBO)

Proposição 1. *Seja X um conjunto não vazio de inteiros positivos, então existe um $x_0 \in X$ tal que $x_0 \leq x$, $\forall x \in X$. Em outras palavras, todo conjunto não vazio de inteiros positivos possui um menor elemento ou elemento mínimo.*

Esse princípio nos ajuda a provar alguns resultados que podem ser interessantes. Mostraremos alguns deles a seguir.

Proposição 2. *A equação $x^3 + 2y^3 = 4z^3$ não possui solução em $\mathbb{N}$.*

Demonstração. Suponha, por absurdo, que exista uma solução e considere o conjunto das soluções como sendo $S = \{z \in \mathbb{N} | 4z^3 = x^3 + 2y^3, x, y \in \mathbb{N}\}$. Como tem solução, $S \neq \emptyset$. Logo, pelo P.B.O, S possui um elemento mínimo. Chamaremos esse elemento de z_1. Portanto, existem $x_1, y_1 \in \mathbb{N}$ tais que

$$4z_1^3 = x_1^3 + 2y_1^3.$$

Note que, então, x_1^3 é um número par, já que podemos escrevê-lo como sendo $x_1^3 = 4z_1^3 - 2y_1^3 = 2(2z_1^3 - y_1^3)$. E, portanto, x_1 é par. Pois se fosse ímpar, seria um número na forma $x_1 = 2n + 1$, ao passo que se elevássemos x_1 ao cubo, ficaria $(2n + 1)^3 = 8n^3 + 12n^2 + 6n + 1$, que é também um número ímpar.

Assim, $x_1 = 2x_2, x_2 \in \mathbb{N}$. Logo,

$$\begin{aligned} 4z_1^3 &= 8x_2^3 + 2y_1^3 \\ \Rightarrow 2z_1^3 &= 4x_2^3 + y_1^3. \end{aligned}$$

Pelo mesmo motivo que x_1, $y_1 = 2y_2, y_2 \in \mathbb{N}$. Logo,

$$\begin{aligned} 2z_1^3 &= 4x_2^3 + 8y_2^3 \\ \Rightarrow z_1^3 &= 2x_2^3 + 4y_2^3. \end{aligned}$$

Repetimos a mesma ideia para provar que z_1 é par e que, portanto, $z_1 = 2z_2, z_2 \in \mathbb{N}$. Logo,

$$\begin{aligned} 8z_2^3 &= 2x_2^3 + 4y_2^3 \\ \Rightarrow 4z_2^3 &= x_2^3 + 2y_2^3. \end{aligned}$$

Isso implica dizer que $z_2 \in S$ e como $z_2 < z_1$ e z_1 é o elemento mínimo de S, então chegamos à uma contradição, o que prova que $S = \emptyset$ e que de fato não existem soluções de números inteiros positivos para a equação $x^3 + 2y^3 = 4z^3$. □

Proposição 3 (Princípio Fundamental da Teoria dos Números)**.** *Não existe número inteiro entre 0 e 1.*

Demonstração. Suponha, por absurdo, que exista um número inteiro entre 0 e 1 e tomemos o conjunto desses números como sendo o conjunto $S = \{x \in \mathbb{Z} | 0 < x < 1\}$. Portanto, S é não vazio. Pelo P.B.O, esse conjunto tem um elemento mínimo, que chamaremos de a. Logo, $0 < a < 1 \Rightarrow 0 < a^2 < a < 1$. Isso implica dizer que $a^2 \in S$ e como $a^2 < a$, contraria a minimalidade de a. Logo, $S = \emptyset$, o que prova a nossa afirmação.

□

Proposição 4. $\sqrt{2} \notin \mathbb{Q}$.

Demonstração. Suponha, por absurdo, que $\sqrt{2} \in \mathbb{Q}$. Logo, o conjunto $S = \{n \in \mathbb{N} | n\sqrt{2} \in \mathbb{Z}$ é não-vazio, pois $\sqrt{2} = \frac{p}{q} \Rightarrow q\sqrt{2} = p \in \mathbb{Z}$.

Pelo P.B.O, existe um elemento minimal $b \in S$. Logo, existe $a \in \mathbb{Z}$, tal que $a = b\sqrt{2} \Rightarrow \sqrt{2} = \frac{a}{b}$

Temos que

$$\begin{aligned} 1 < \sqrt{2} < 2 \\ \Rightarrow 1 < \frac{a}{b} < 2 \\ \Rightarrow 0 < \frac{a}{b} - 1 < 1 \\ \Rightarrow 0 < a - b < b. \end{aligned}$$

Por outro lado, temos que

$$\begin{aligned} \sqrt{2} = \frac{2 - \sqrt{2}}{\sqrt{2} - 1} = \frac{2 - \frac{a}{b}}{\frac{a}{b} - 1} = \frac{2b - a}{a - b} \\ \Rightarrow (a - b)\sqrt{2} = 2b - a \in \mathbb{Z} \end{aligned}$$

$$\Rightarrow (a-b) \in S.$$

O que é uma contradição, já que $(a-b) < b$ e b é o elemento mininmal de S. Ou seja, $S = \emptyset$ e, portanto, $\sqrt{2} \notin \mathbb{Q}$.

□

4.2 Principio da Indução Finita

Outra consequência do Principio da Boa Ordenação é o que chamamos de Princípio da Indução, que pode ser posto de duas formas:

Proposição 5 (**Principio da Indução Finita(1° forma)**). *Seja $X \subset \mathbb{N}$, se $1 \in X$ e $n+1 \in X$, sempre que $n \in X$, então $X = \mathbb{N}$.*

Proposição 6 (**Principio da Indução Finita(2° forma)**). *Seja $X \subset \mathbb{N}$, se $1 \in X$ e $n \in X$, sempre que $k \in X$, para todo $1 \leq k < n$, então $x = \mathbb{N}$.*

Teorema 4.2.1. *O Principio da Boa Ordenação e as duas formas do Princípio da Indução Finita são equivalentes.*

Demonstração.

1. (Proposição 5 ⇒ Proposição 6)

   Seja $X \subset \mathbb{N}$ tal que $1 \in X$ e $n+1 \in X$ sempre que $k \in X$, para todo $1 \leq k < n+1$. Queremos mostrar que $X = \mathbb{N}$.

   Sabemos que se $1 \in X$ e $n+1 \in X$ sempre que $n \in X$, então $X = \mathbb{N}$.

   Temos que $1 \in X$. Seja $n \in X$. Queremos mostrar que $n+1 \in X$. Suponha, por absurdo, que $n+1 \notin X$.

   Portanto, existe $p_0 < n$ tal que $p_0 \notin X$, pois, caso contrário, $n+1$ também pertenceria a X. Analogamente, existe $p_1 < p_0$ tal que $p_1 \notin X$.

   Seguindo esses passos sucessivamente, mostramos que $1 \notin X$, o que é uma contradição. Logo, $n+1 \in X$ e, pela Proposição 5, $X = \mathbb{N}$.

2. (Proposição 6 ⇒ Proposição 1)

   Seja $X \subset \mathbb{N}$ não-vazio. Queremos mostrar que X possui elemento mínimo. Se $X = \mathbb{N}$, então X tem elemento mínimo.

   Vamos supor que o conjunto $Y = \mathbb{N} - X$ é não vazio. Se $1 \in X$ mais uma vez, X tem elemento mínimo. Suponha que $1 \notin X$. Logo, $1 \in Y$. se X não possui elemento mínimo, podemos concluir que $2 \notin X$, $3 \notin X$, ... Podemos afirmar que até um

$n \in \mathbb{N}$, $k \notin X$, para todo $1 \leq k < n$. Porém, $n \notin X$, pois, caso contrário, n seria o elemento minimal de X. Logo, $n \in Y$ sempre que $k \in Y$, para todo $1 \leq k < n$.

Pela Proposição 6, $Y = \mathbb{N}$ e $X = \emptyset$, o que é uma contradição. Logo, X tem elemento mínimo.

3. (Proposição 1 $\Rightarrow$ Proposição 5)

   Seja $X \subset \mathbb{N}$ tal que $1 \in X$ e $n + 1 \in X$ sempre que $n \in X$. Queremos mostrar que $X = \mathbb{N}$.

   Vamos supor que o conjunto $Y = \mathbb{N} - X$ é não vazio. Note que $1 \notin Y$. Temos, pelo P.B.O, que Y possui elemento mínimo. Chamemos de n_0 esse elemento.

   Como $n_0 \neq 1$, então existe n tal que $n_0 = n + 1$. Como $n < n_0$, $n \notin Y$ e $n \in X$. Mas, então, $n + 1 = n_0 \in X$, o que é uma contradição. Logo, $X = \mathbb{N}$.

□

4.3 Divisibilidade e Máximo Divisor Comum

Falaremos agora sobre algumas definições importantes sobre os números inteiros, sendo a primeira delas a de divisibilidade

Definição 1 (**Divisibilidade**). *Sejam a e $b \in \mathbb{Z}$, com $a \neq 0$. Dizemos que b é múltiplo de a ou que a divide b se existir um inteiro c tal que $b = ac$, e usamos como notação $a \mid b$. Se a não divide b, então denotamos por $a \nmid b$.*

Proposição 7 (**Algumas regras de números inteiros**). *Tomemos a, b e $c \in \mathbb{Z}$. Então:*

1. *$a \mid 0$ e $a \mid a$*
2. *Se $a \mid b$ e $b \mid c$, então $a \mid c$*
3. *$a \mid b$ e $a \mid c$, então $a \mid (b + c)$ e $a \mid (b - c)$*
4. *Se a e b são positivos e $a \mid b$, então $0 < a \leq b$*

Demonstração.

1. Como podemos escrever o número 0 como $0 = a.0$ e a como $a = a.1$, então segue da definição de divisibilidade que $a \mid 0$ e $a \mid a$.

2. Como, pela definição de divisibilidade, $b = ar$ e $c = bt$, então podemos escrever

$$c = (ar)t$$

$$\Rightarrow c = a(rt)$$

$$\Rightarrow a \mid c.$$

3. De fato, se $a \mid b$ e $a \mid c$, então $b = ar_1$ e $c = ar_2$. Somando $b + c$, temos:

$$b + c = ar_1 + ar_2$$

$$\Rightarrow b + c = a(r_1 + r_2)$$

$$\Rightarrow a \mid (b + c).$$

De forma análoga, prova-se que

$$a \mid (b - c).$$

4. Se a e b são positivos e $a \mid b$, então $b = ar$, com $r \geq 1$. Podemos multiplicar por essa desigualdade por a, obtendo:

$$ar \geq a1$$

$$\Rightarrow ar \geq a.$$

E como $b = ar$, então:

$$b = ar \geq a \geq 0.$$

Ou seja, $0 < a \leq b$.

□

Teorema 4.3.1 (**Algoritmo da Divisão**). *Sejam a e b inteiros positivos. Então, existem números inteiros únicos q e r tais que $a = bq + r$, com $0 \leq r < b$.*

Demonstração. Existência:

Dados $a, b \in \mathbb{Z}$, com $b > 0$, considere o conjunto $S = \{a - bx | x \in \mathbb{Z}, 0 \leq a - bx\}$. Temos que $S \subset \mathbb{N}$.

Para $x = -|a|$, temos

$$a - bx = a - b(-|a|) = a + b|a|.$$

E como $1 \leq b$, então

$$0 \leq a + |a| \leq a + b|a|.$$

Isso mostra que $S \neq \emptyset$. Pelo P.B.O, existe um elemento mínimo $r \in S$. Portanto, existe $x = q \in \mathbb{Z}$ tal que $r = a - bq \Rightarrow a = bq + r$. Faltar provar que $0 \leq r < b$.

Suponha $b \leq r$. Então $0 \leq r - b = a - bq - b \Rightarrow r > a - (q+1)b \in S$, o que contradiz a minimalidade de r. Ou seja, $b \leq r$ é impossível. Portanto, $r < b$.

Unicidade:

Suponha que $q, r, k, h \in \mathbb{Z}$ tais que $a = bq + r = bk + h$, com $0 \leq r, h < b$. Então $h - r = bq - bk = b(q - k)$. Daí segue que $|h - r| = |b(q - k)| = b|q - k|$.

Somemos agora as desigualdades $0 \leq h < b$ e $-b < -r \leq 0$ e teremos o resultado $-b < h - r < b$, ou seja, $|h - r| < b$. Temos então a contradição, no caso de $q \neq k$:

$$b \leq |h - r| = b|q - k| < b.$$

Assim, $q = k$ e, portanto, $r = h$.

□

Outra definição que nos auxiliará daqui para frente é a de máximo divisor comum. Para entendermos o que é o máximo divisor comum, porém, precisamos primeiro definir o que é um divisor comum. De forma simples, sejam a, $b \in \mathbb{Z}$. Dizemos que d é um divisor comum de a e b se $d \mid a$ e $d \mid b$. Ou seja, o divisor comum de dois números é um número que divide os dois ao mesmo tempo.

A partir disso, podemos enunciar a definição de máximo divisor comum como sendo:

Definição 2 (**Máximo divisor comum**). *Sejam a, b, $d \in \mathbb{Z}$, então d é máximo divisor comum entre a e b, e é denotado como $mdc(a, b) = d$, se $d \mid a$ e $d \mid b$, para todo $c \in \mathbb{Z}$ tal que $c \mid a$ e $c \mid b \Rightarrow c \mid d$.*

Como exemplo, os números 20 e 16 possuem como divisores em comum: -4, -2, -1, 1, 2, 4. Dentre esses, o máximo divisor comum de 20 e 16 é 4. Também pode ser escrito como $mdc(20, 16) = 4$.

Para encontrarmos o *mdc* entre dois números inteiros, existe um método simples e eficiente: o algoritmo de Euclides. Antes, porém, de enunciarmos esse importante resultado, veremos um lema que nos ajudará no entendimento dele:

Lema 4.3.2. *Sejam a e $b \in \mathbb{Z}$. Se existem q e r, também inteiros, tais que $a = bq + r$, então o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r. Nesse caso, vale notar então que $mdc(a, b) = mdc(b, r)$.*

Demonstração. Seja c um divisor comuum qualquer de a e b. Ou seja, $a = cx$ e $b = cy$. Portanto, podemos reescrever a equação $a = bq + r$, como sendo

$$
\begin{aligned}
cx &= (cy)q + r \\
\Rightarrow cx - (cy)q &= r \\
\Rightarrow r &= c(x - yq) \\
\Rightarrow c|r.
\end{aligned}
$$

□

Teorema 4.3.3 (**Algoritmo Euclidiano**). *Dados dois inteiros positivos a e b, aplicamos o algoritmo da divisão sucessivas vezes para obter o máximo divisor comum entre esses dois números. Ao fazer isso, encontramos a seguinte sequência de igualdades:*

$$
\begin{cases}
b = aq_1 + r_1, & 0 \leq r_1 < a \\
a = r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\
r_1 = r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\
r_2 = r_3q_4 + r_4, & 0 \leq r_4 < r_3 \\
\vdots & \\
r_{n-2} = r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} = r_nq_{n+1} &
\end{cases}
$$

E o $mdc(a, b)$ é o último resto não nulo da nossa sequência de divisões, ou seja, r_n.

Demonstração. Podemos observar que a sequência de restos $r_k \in \mathbb{Z}$ é estritamente decrescente (os restos se tornam cada vez menores) e são limitados por $0 \leq r_k < a$. Examinando, então, a sequência de igualdades exposta acima, usando como base o lema anterior, temos que:

$$mdc(a, b) = mdc(a, r_1) = mdc(r_1, r_2) = mdc(r_2, r_3) = \cdots = mdc(r_{n-1}, r_n) = r_n$$

□

Teorema 4.3.4 (**Algoritmo Euclidiano Estendido**). *Sejam a e b inteiros positivos e seja d o máximo divisor comum entre eles. Então existem k e $g \in \mathbb{Z}$ tais que*

$$ax_1 + by_1 = d.$$

Demonstração. Considere o conjunto $S = \{ax + by | x, y \in \mathbb{Z}, 0 < ax + by\}$. Seja primeiro $a \neq 0$. Fazendo-se $y = 0$ e $x = 1$ para o caso de $0 < a$, e $x = -1$ para o caso de $a < 0$, temos que $ax + by = |a| + b.0 = |a| > 0$, o que mostra que $S \neq \emptyset$. Se $a = 0$, então $|b| > 0$ e escolhendo-se analogamente x e y, mostra-se que $S \neq \emptyset$ também neste caso.

Pelo P.B.O, existe um elemento minimal $d > 0 \in S$. Portanto, existem $x_1, y_1 \in \mathbb{Z}$ tais que $d = ax_1 + by_1$. Afirmamos que d é o $mdc(a, b)$. Agora dividamos a por d com resto. Ou seja, existem $q, r \in \mathbb{Z}$ tais que $a = qd + r$, com $0 \leq r \leq< d - 1 < d$. Então $r = a - qd = a - q(ax_1 + by_1) = a(1 - qx_1) + b(-qy_1)$. Se $r > 0$, poderíamos concluir que $r \in S$, o que absurdo, dado que $r < d$ e d é o elemento minimal de S. Então $r = 0$ e $a = qd$, o que significa que $d \mid a$. Analogamente, mostra-se que $d \mid b$. Logo, d é divisor comum de a e b. Falta-nos provar que d é o maior dos divisores comuns de a e b.

Seja $c \in \mathbb{N}$ tal que $c \mid a$ e $c \mid b$. Pela proposição 6, temos que $c \mid ax_1 + by_1 = d$. Ou seja, $c \mid d \Rightarrow mdc(a, b) = d$. □

Definição 3 (**Números primos entre si**). *Dois números $a, b \in \mathbb{Z}$ são chamados primos entre si ou relativamente primos, se $mdc(a, b) = 1$.*

Por exemplo, os números -7 e 5 são primos entre si, pois o $mdc(-7, 5) = 1$.

Proposição 8. *Dois números $a, b \in \mathbb{Z}$ são relativamente primos se, e somente se existem $x_1, y_1 \in \mathbb{Z}$ tais que*

$$ax_1 + by_1 = 1.$$

Demonstração.

1. ($\Rightarrow$)

   Seja $d = mdc(a, b)$. Se $d = 1$, existem os $x_1, y_1 \in \mathbb{Z}$ tais que $ax_1 + by_1 = 1$, pelo Algoritmo Euclidiano Estendido.

2. ($\Leftarrow$)

   Seja $ax + by = 1$ possível com $x, y \in \mathbb{Z}$. Como $d|a$ e $d|b$, então $d|1$, o que implica que $d = 1$.

□

Lema 4.3.5. *Sejam a, b e $c \in \mathbb{Z}_+$ e sejam a e b primos entre si. Então:*

1. *Se b divide o produto ac, então b divide c*
2. *Se a e b dividem c, então o produto ab divide c*

Demonstração.

1. Como a e b são primos entre si, então $mdc(a, b) = 1$. Pelo Algoritmo de Euclides Estendido, podemos afirmar que existem k_1 e k_2 tais que $k_1a+k_2b = 1$. Multiplicando ambos os lados dessa equação por c, obtemos:

$$k_1ac + k_2bc = c$$

E como $b \mid ac$ e $b \mid b$, então $b \mid k_1ac + k_2bc$. Ou seja,

$$b \mid c.$$

2. Como $a \mid c$, então $at = c$, para algum $t \in \mathbb{Z}$. Além disso, como b também divide c e $mdc(a, b) = 1$, então $b \mid t \rightarrow t = bk$, sendo $k \in \mathbb{Z}$. Assim, temos:

$$\begin{aligned} & at = c \\ \Rightarrow & a(bk) = c \\ \Rightarrow & (ab)t = c \end{aligned}$$

Portanto,

$$ab \mid c.$$

□

Entendidos esses conceitos, falaremos agora sobre a definição de números primos e do Teorema fundamental da Aritmética, para depois elucidar os conceitos da aritmética modular e, só então, poderemos entender o funcionamento do método RSA.

4.4 Números primos e o Teorema Fundamental da Aritmética

Definição 4 (**Números primos**). *Um número $p \in \mathbb{N}$ é chamado primo se satisfaz as seguintes condições:*

1. $p > 1$;
2. *Os únicos divisores de p são:* 1 *e* p.

Indicamos o conjunto dos números primos por $\mathbb{P} = \{p \in \mathbb{N} | \text{p é primo}\}$. Se p não é primo, então é dito composto.

Antes de enunciarmos o Teorema Fundamental da Aritmética, veremos mais um Lema que ajuda no entendimento deste:

Lema 4.4.1 (**Lema de Euclides**). *Seja $p \in \mathbb{P}$ e $a, b \in \mathbb{Z}_+$. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$. Ou seja, um número primo divide um produto, somente se ele divide um dos fatores.*

Demonstração. Se $p \mid ab$, então existe $c \in \mathbb{Z}$ tal que $ab = pc$. Suponhamos que $p \nmid a$, ou seja, $mdc(p, a) = 1$. Isso significa que existem k_1 e $k_2 \in \mathbb{Z}$ tais que

$$ak_1 + pk_2 = 1$$

Multiplicando ambos os lados dessa equação por b, obtemos:

$$abk_1 + pbk_2 = b$$

E como, por hipótese, $p \mid ab$ e $p \mid p$, então

$$p \mid abk_1 + pbk_2$$

Ou seja

$$p \mid b$$

De forma análoga, provamos que, se $p \nmid b \Rightarrow p \mid a$.

□

Tendo em mãos o lema anterior e o Lema 4.3.5, enunciaremos o seguinte teorema:

Teorema 4.4.2 (**Teorema Fundamental da Aritmética**). *Dado um $n \in \mathbb{Z}$, com $n \geq 2$, podemos sempre escrevê-lo de modo único, na forma:*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} ... \cdot p_k^{\alpha_k}$$

Onde os p_k, com $1 \leq k \leq \infty$, tais que $1 < p_1 < p_2 < ... < p_k$ são números primos e α_1, α_2, α_3, ..., α_k são inteiros positivos.

Demonstração. Existência.

Seja $n \in \mathbb{Z}$ maior que 1. Denotando por p_1 seu menor divisor primo, tem-se que

$$n = p_1 f_1, \qquad 1 \leq f_1 < n$$

Se $f_1 = 1$, então $n = p_1$ e, portanto, obtêm-se a fatoração desejada. Caso contrário, denotando por p_2 o menor número primo que é fator de f_1, tem-se que $f_1 = p_2 f_2$. Ou seja,

$$n = p_1 p_2 f_2 \qquad 1 \leq f_2 < f_1$$

Se $f_2 = 1$, então $n = p_1p_2$ e, de novo, obtêm-se a fatoração desejada. Caso contrário, denotando por p_3 o menor número primo que é fator de f_2, tem-se que $f_2 = p_3f_3$. Ou seja,

$$n = p_1p_2p_3f_3 \qquad 1 \leq f_3 < f_2 < f_1$$

Assim, continuamos esse processo sucessivamente, obtendo uma sequência estritamente decrescente de números inteiros positivos:

$$n > f_1 > f_2 > f_3 > ... > f_n > f_{n+1} > ... \geq 1$$

Então, existe uma quantidade finita de índices n, de tal modo que $f_n > 1$ e, consequentemente, $f_{n+1} = 1$, de onde segue que $n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n$.

Como os números p podem se repetir, então podem aparecer potências de alguns deles, produzindo a notação usada ao enunciarmos o teorema.

Unicidade

Suponhamos, por absurdo, que um inteiro positivo $n \geq 2$ possua duas fatorações distintas:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} ... \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} ... \cdot q_s^{\beta_s}.$$

Onde, $1 < p_1 < p_2 < ... < p_k$ e $1 < q_1 < q_2 < ... < q_s$ são primos e α_1, α_2, α_3, ..., α_k e β_1, β_2, β_3, ..., α_s são inteiros positivos.

Como $p_1 \mid n$, então p_1 deve dividir os fatores do produto à direita. Mas, sendo p_1 um número primo, então só pode dividir outro se forem iguais. Então $p_1 = q_j$ para algum $j \in \mathbb{Z}$ entre 1 e s. Logo,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} ... \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} ... \cdot q_j^{\beta_j} \cdot ... \cdot q_s^{\beta_s}$$

$$= q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} ... \cdot p_1^{\beta_j} \cdot ... \cdot q_s^{\beta_s}.$$

Cancelando então p_1 em ambos os lados da equação, ficamos com

$$n = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} ... \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot q_3^{\beta_3} ... \cdot p_1^{\beta_j - 1} \cdot ... \cdot q_s^{\beta_s} = x.$$

Sendo x um número menor que n que possui duas fatorações únicas, o que é um absurdo, pois contraria a minimalidade de n. Portanto, a fatoração é única.

□

Falaremos, no seguinte capítulo, sobre a última parte teórica necessária para compor o método de criptografia RSA, a aritmética modular.

5 Aritmética modular

Primeiro, relembremos o que é a relação de equivalência.

Definição 5 (**Relação de Equivalência**). *Seja X um conjunto qualquer onde está definida uma relação que denotaremos por $\sim$. Essa relação é chamada relação de equivalência se, para quaisquer x, y, $z \in \mathbb{Z}$, satisfaz as seguintes propriedades:*

1. *$\sim$ é reflexiva, ou seja, $x \sim x$;*
2. *$\sim$ é simétrica: se $x \sim y$, então $y \sim x$*
3. *$\sim$ é transitiva: se $x \sim y$ e $y \sim z$, então $x \sim z$*

Agora, construiremos uma relação de equivalência para o conjunto dos números inteiros, $\mathbb{Z}$.

Definição 6 (**Congruência**). *Sendo $m \in \mathbb{N}$ e a e b inteiros quaisquer, dizemos que a é congruente a b módulo m se os restos das divisões de a e b por m são iguais.*

Como notação, usa-se $a \equiv b \pmod{m}$ (lê-se "a é congruente a b módulo m").

Como exemplo, podemos escrever que $15 \equiv 8 \pmod{7}$ ou ainda que $8 \equiv -6 \pmod{7}$

Dessa definição, segue o resultado:

Proposição 9. *Dizemos que a é congruente a b módulo m se, e somente se m é um múltiplo da diferença entre a e b.*

Demonstração.

1. ($\Rightarrow$)

   Primeiro, faremos as divisões euclidianas de a e b por m, obtendo $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leq r_1, r_2 < m$. Como $a \equiv b \pmod{m}$, então $r_1 = r_2$. Subtraindo, então, as duas equações, obtemos:

$$\begin{aligned} a - b &= mq_1 - mq_2 + r_1 - r_2 \\ \Rightarrow a - b &= m(q_1 - q_2) + (r_1 - r_2) \\ \Rightarrow a - b &= m(q_1 - q_2) \\ \Rightarrow m &| (a - b). \end{aligned}$$

2. ($\Leftarrow$)

   Como $m|(a-b)$ e $a-b = m(q_1-q_2)+(r_1-r_2)$, então $m|(r_1-r_2)$.

   Por outro lado, como $0 \leq r_1, r_2 < m$, então $-m < (r_1-r_2) < m$. Ou seja, $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$. E, portanto, $a \equiv b \pmod{m}$.

□

Como 0 é múltiplo de qualquer número inteiro por definição, então $a - a = 0$ é múltiplo de m. Ou seja, $a \equiv a \pmod{m}$

Podemos notar que se $a \equiv b \pmod{m}$, então, como vimos, $(a-b) = mk$. Se multiplicarmos ambos os lados por -1, teremos $(b-a) = mh$, com $h = -k$. Ou seja, $(b-a)$ é também um múltiplo de m e, portanto, $b \equiv a \pmod{m}$.

Observa-se ainda que, se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então tanto $(a-b)$ quanto $(b-c)$ são múltiplos de n. Ao somarmos esses dois números, ficamos com:

$$\begin{aligned}(a-b)+(b-c) &= mk+mh \\ \Rightarrow (a-c) &= mk+mh \\ \Rightarrow (a-c) &= m(k+h)\end{aligned}$$

E, portanto, $a \equiv c \pmod{m}$.

Ou seja, a congruência é uma relação de equivalência: é reflexiva, simétrica e transitiva.

Abaixo, listaremos algumas propriedades da congruência, em forma de teorema:

Teorema 5.0.1. *Seja $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:*

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ka \equiv kb \pmod{m}, k \in \mathbb{Z}$
4. $ac \equiv bd \pmod{m}$
5. $a^k \equiv b^k \pmod{m}$

Demonstração.

1. Por hipótese, $a = mh_1 + b$ e $c = mh_2 + d$. Realizando a soma $a + c$, ficamos com:

$$a + c = mh_1 + b + mh_2 + d$$
$$\Rightarrow a + c = m(h_1 + mh_2) + (b + d)$$

   Ou seja,

$$a + c \equiv b + d \pmod{m}$$

2. Análogo ao primeiro item.

3. Como, por hipótese, $a = mh_1 + b$, se multiplicarmos ambos os lados por k, obtemos:

$$ak = mh_1k + bk$$
$$\Rightarrow ak - bk = m(h_1k)$$

   E, portanto:

$$ka \equiv kb \pmod{m}$$

4. A prova será parecida a do item 1. Realizando a multiplicação ac, temos:

$$ac = (mh_1 + b)(mh_2 + d)$$
$$\Rightarrow ac = mh_1mh_2 + mh_1d + bmh_2 + bd$$
$$\Rightarrow ac = m(h_1h_2m + h_1d + bh_2) + bd$$

   Portanto,

$$ac \equiv bd \pmod{m}$$

5. Pela propriedade 4, $ac \equiv bd \pmod{m}$, temos que se $a \equiv b \pmod{m}$ então $aa \equiv bb \pmod{m}$. Ainda pela mesma razão, $aaa \equiv bbb \pmod{m}$. Se repetirmos esse processo k vezes, obtemos

$$a^k \equiv b^k \pmod{m}.$$

Terminando, assim, nossa demonstração. □

Mostraremos os teoremas de Fermat e Euler, muito importantes para o método RSA. Antes, porém, enunciaremos um outro teorema que servirá de suporte para as definições seguintes.

Teorema 5.0.2. *Se a, b, c e m são números inteiros e $ac \equiv bc \pmod{m}$, então $a \equiv b \pmod{\frac{m}{d}}$, onde $d = mdc(c, m)$.*

Demonstração. Sendo $ac \equiv bc \pmod{m}$, então $ac - bc = c(a-b) = km$. Se dividirmos os dois membros por d, teremos $\frac{c}{d}(a-b) = k(\frac{m}{d})$. Logo, $\frac{m}{d} | \frac{c}{d}(a-b)$ e como $mdc(\frac{m}{d}, \frac{c}{d}) = 1$, então $\frac{m}{d} | (a-b)$, o que implica $a \equiv b \pmod{\frac{m}{d}}$.

□

Teorema 5.0.3 (**Pequeno Teorema de Fermat**). *Seja p um número primo e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então $a^{p-1} \equiv 1 \pmod{p}$*

Demonstração. Para começarmos essa demonstração, consideremos a sequência $\{a, 2a, ..., (p-1)a\}$. Esta é uma sequência de $(p-1)$ múltiplos de a em que não há múltiplos de p: consideremos os índices que multiplicam nossa sequência como um número $k \in \{1, 2, 3, ..., (p-1)\}$. Como, para qualquer valor de k, $k < p$ e $p \nmid a$, então $p \nmid ka$. Ou seja, de fato não existem múltiplos de p em nossa lista.

Além disso, nessa lista não há dois números diferentes que sejam congruentes módulo p, pois se existissem, então dados $k_1, k_2 \in \{1, 2, 3, ..., (p-1)\}$, com $k_1 \neq k_2$,

$$\begin{aligned} ak_1 &\equiv ak_2 \pmod{p} \\ \Rightarrow k_1 &\equiv k_2 \pmod{p} \end{aligned}$$

Mas como $k_1, k_2 \in \{1, 2, 3, ..., (p-1)\}$ e são congruentes, então $k_1 = k_2$, o que contradiz nossa hipótese, provando o que queríamos.

Por conta disso, cada um dos números da sequência é congruente à $1, 2, 3, ..., (p-1)$. Isso nos leva ao último passo de nossa demonstração, que consiste em multiplicar todos os termos de nossa sequência original:

$$\begin{aligned} a \cdot 2a \cdot 3a \cdot ... \cdot (p-1) &\equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \pmod{p} \\ \Rightarrow a^{p-1} \cdot (p-1)! &\equiv (p-1)! \pmod{p} \\ \Rightarrow a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

Terminando, assim, nossa demonstração.

□

Definição 7 (**Função ϕ de Euler**). *Seja $m \in \mathbb{N}$. Definiremos a função $\phi(m)$ como sendo o número de inteiros positivos entre 1 e $m-1$ que são co-primos com m.*

E daí, podemos anunciar o teorema de Euler da seguinte maneira:

Teorema 5.0.4 (**Teorema de Euler**). *Seja $m, a \in \mathbb{Z}$ primos entre si, então*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Demonstração. Considere o conjunto dos restos co-primos com m, $S = \{r_1, r_2, ..., r_{\phi(m)}\}$. E agora considere um conjunto $L = \{ar_1, ar_2, ..., ar_{\phi(m)}\}$, ou seja, o conjunto que tem os mesmo elementos de S, porém multiplicados por a.

Note que cada elemento do conjunto L é co-primo com m, dado que tanto a quanto cada resto r_i, com $i = 1, 2, ..., \phi(m)$, são co-primos com m. Então o resto de cada elemento de L na divisão por m é um elemento de S, pois é um resto co-primo com m. Além disso, os dois conjuntos tem a mesma cardinalidade, ou seja, cada elemento de S aparece exatamente uma vez em L.

Para provarmos isso, vamos supor, por absurdo, que existem 2 elementos diferentes em L que possuem restos iguais na divisão por m. Então se $ar_i \equiv ar_j \pmod{m}$, com $i, j = 1, 2, ..., \phi(m)$, e como a é co-primo com m, podemos simplificá-lo na congruência, ficando com $r_i \equiv r_j \pmod{m} \Rightarrow i = j$.

Como consequência desse fato, temos:

$$r_1 \cdot r_2 \cdot ... \cdot r_{\phi(m)} \equiv ar_1 \cdot ar_2 \cdot ... \cdot ar_{\phi(m)} \pmod{m}$$
$$\Rightarrow r_1 \cdot r_2 \cdot ... \cdot r_{\phi(m)} \equiv a^{\phi(m)} \cdot r_1 \cdot r_2 \cdot ... \cdot r_{\phi(m)} \pmod{m}$$

E como cada um dos restos é primo com m, então o produto de todos eles também é. Assim, podemos simplificá-los na equivalência, obtendo:

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

□

6 Método de criptografia RSA

Relembrados todos os conceitos matemáticos necessários, podemos então descrever como funciona o método de criptografia RSA e entender o porque de ser um método seguro e amplamente usado até hoje. Antes disso, porém, falaremos sobre algumas características acerca dos números primos, números esses que constituem a base do método.

6.1 Carecterísticas dos números primos

Como já vimos neste trabalho, os números primos são números naturais que só possuem um divisor próprio ou, em outras palavras, são os números naturais que só são divisíveis por 1 e por eles mesmos. É interessante notar que o número 2 é o único número primo par, pois todos os outros naturais pares são divisíveis por 1, por eles mesmos e por 2.

Dos mistérios e propriedades interessantes que envolvem esses números e instigam os cientistas há tantos anos, enunciaremos alguns abaixo, sendo o primeiro deles dado à Euclides:

Teorema 6.1.1. *Existem infinitos números primos.*

Demonstração. Vamos supor, por absurdo, que a quantidade de números primos seja finita. Portanto, existe um número primo p tal que p é o maior número primo existente. Agora, seja

$$q = 2 \cdot 3 \cdot ... \cdot p + 1.$$

Ou seja, q é igual ao produto de todos os números primos até p, somado com 1. Se provarmos que q é um número primo, nossa suposição de que existem finitos números primos será falsa, dado que q é claramente maior do que p e, assim, provaremos que existem infinitos primos.

Bom, sendo $q = 2 \cdot 3 \cdot ... \cdot p + 1$, então q não é divisível por 2, pois $2 \cdot 3 \cdot ... \cdot p$ é um número divisível por 2, o que faz dele um número par. Ao somarmos 1 à $2 \cdot 3 \cdot ... \cdot p$, teremos então um número ímpar, que não é divisível por 2. Da mesma forma, $2 \cdot 3 \cdot ... \cdot p$ é um múltiplo de 3 e, ao somar 1 à esse número, o resultado não é mais divisível por 3.

Usando raciocínio análogo, podemos chegar à conclusão que nenhum dos números de 2 até p dividem o número q e, portanto, seus únicos divisores são o 1 e o próprio q, o que faz dele um número primo e isso contradiz nossa suposição. Assim, fica provado que existem infinitos números primos. □

O fato de que existem infinitos números primos deles deixa claro que existem números primos muito grandes. Esse resultado, combinado com o teorema fundamental da aritmética, é o que faz do método RSA um método muito seguro de criptografia.

Apesar da comprovação de que existem infinitos primos, esses números não obedecem uma distribuição padronizada e isso significa que existem intervalos de números naturais que não possuem nenhum número primo. Poderíamos montar uma lista de números naturais consecutivos compostos com 5 números, por exemplo? A resposta seria sim, basta tomarmos a lista 24, 25, 26, 27 e 28. E se quisermos montar uma lista assim, porém com mais números? É o que o teorema abaixo nos garante.

Teorema 6.1.2. *É possível criar uma lista com o tamanho que se queira de números compostos consecutivos.*

Para isso, escolhemos um número natural n maior do que 1 e calculamos $m = n(n+1)(n+2)(n+3)...(n+(k-1))+n$, onde k é a quantidade de termos de nossa sequência. Esse número m será o primeiro número de nossa lista.

Por exemplo, se quisermos fazer uma lista com 3 números não primos consecutivos e escolhermos $n = 6$, teremos $m = 2(6+1)(6+2)+6 = 118$. Portanto, nossa lista, nesse caso, seria: 118, 119, 120.

Demonstração. Peguemos o número

$$m = n(n+1)(n+2)(n+3)+n.$$

Neste caso, m é divisível por n e como $n > 1$, então m não é primo. Para o número consecutivo à m, temos

$$n(n+1)(n+2)(n+3)+(n+1)$$

que é divisível por $(n+1)$, o que garante que não é primo também. Se repetirmos esse processo, provamos que os k números consecutivos de nossa lista não são primos e, portanto, conseguimos construir uma lista de qualquer tamanho em que todos seus elementos são números compostos consecutivos. □

Podemos mencionar ainda que existem problemas que há muito incomodam os cientistas matemáticos e que seguem sem comprovação. Enunciaremos duas dessas conjecturas, que são mais dois pontos que jogam luz nos mistérios que envolvem os números primos. Apesar de podermos criar uma lista de qualquer tamanho de números consecutivos sendo todos eles números compostos, Euclides fez a seguinte conjectura:

Conjectura 1. *Existem infinitos números primos gêmeos.*

Definição 8 (**Primos gêmeos**). *Dois números $p_1, p_2 \in \mathbb{P}$ são ditos gêmeos se $p_2 = p_1+2$.*

Ou seja, existem infintos pares de números primos "próximos" um do outro.

Como exemplo, podemos citar os pares de primos gêmeos (3,5) e (11,13). O último primo gêmeo encontrado, em setembro de 2016, tem mais de 300 mil dígitos. Esses resultados trazem à luz a imprevisibilidade dos números primos.

A segunda conjectura que veremos é dada a Christian Goldbach e pode ser escrita como:

Conjectura 2. *Todo número par $4 < n$ é soma de dois primos ímpares.*

Exemplo: $6 = 3 + 3$, $10 = 7 + 3$, $22 = 17 + 5$, ...

Por serem números que possuem características tão únicas e interessantes, os números primos sempre foram e continuam sendo de grande interesse para os pesquisadores, principalmente números primos grandes - números com aproximadamente 300 mil dígitos. Até porque, quanto maiores forem os primos usados para a criptografia, mais difícil se torna descriptografar mensagens no dia de hoje.

Apesar de sua distribuição não ter um padrão definido, existe um resultado muito importante, chamado Teorema dos números primos, que os dá uma boa aproximação do comportamento dos números primos, que enunciaremos depois da definição seguinte. Esse teorema foi provado por Jacques Hadamart Charles-Jean de La Vallée Poussin em 1896, de forma independente. Não colocaremos esta demonstração neste trabalho, pois se trata de uma demonstração envolvendo conceitos que vão além dos trabalhados aqui.

Definição 9. *Para todo $0 \leq x \in \mathbb{R}$ define-se a função $\pi(x)$ como sendo:*

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

Ou seja, $\pi(x)$ é a quantidade de números primos que são menores ou iguais a x.

Por exemplo, $\pi(10) = 4$, pois os números primos menores que 10 são: 2, 3, 5 e 7.

Teorema 6.1.3 (**Teorema dos Números Primos**). *A quantidade de números primos menores ou iguais a x, dado x grande, tem aproximação cada vez melhor por $\dfrac{x}{\ln x}$. Ou seja,*

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

Ou seja, esse teorema trata do comportamento assintótico da função π, mostrando a quantidade de números primos existentes até determinado $x \in \mathbb{R}$. Quanto maior o

número x escolhido, mais preciso será o valor encontrado para a quantidade de números primos até x.

Se, por exemplo, quisermos saber a quantidade de números primos que existem até cem trilhões (100000000000000), pelo Teorema dos Números Primos, obtemos resposta igual a 3.1 trilhões. Esse resultado tem uma precisão maior que 99%, sendo o valor real da contagem próximo à 3.2 trilhões.

Veremos, agora, como se dá todo o processo de codificação e decodificação do método RSA.

6.2 Pré codificação

O método de criptografia RSA é um método chamado de método de chave pública ou chave assimétrica, o que significa dizer que a chave utilizada para codificar a mensagem é pública, estando disponível para qualquer pessoa acessar, enquanto a chave usada para descriptografar a mensagem é privada (cada pessoa possui uma chave pública e uma privada).

Uma pergunta que pode surgir em relação a isso é: Por quê utilizar uma chave pública? Isso não torna a decodificação da mensagem mais fácil? E a resposta é na verdade bem simples. Quando se utiliza um método de chave simétrica, dentre os defeitos encontrados já mencionados nesse trabalho, existe o fato de que, para que o remetente da mensagem e o destinatário possam se comunicar, é necessário que os dois combinem uma chave que vai tanto codificar quanto decodificar a mensagem e isso pode ser um problema: primeiro porque, de alguma maneira, um dos dois tem que entrar em contato com o outro para de fato combinarem a chave, o que abre a possibilidade de uma pessoa indesejada ter acesso a isso, e segundo porque esse fato impossibilita que o remetente mande uma mensagem para o destinatário a qualquer momento.

E é justamente por causa disso que se utiliza chaves públicas e privadas no método RSA: sabendo a chave pública do destinatário, eu posso codificar minha mensagem e enviá-la para ele a qualquer momento, sem precisar combinar uma chave previamente, e de modo que somente o próprio destinatário consegue decifrá-la, usando sua chave privada. Isso torna a comunicação entre os polos da mensagem muito mais rápida. Além dessa vantagem, métodos de criptografia de chave assimétrica também aumentam a segurança do sigilo, uma vez que somente a chave privada precisa ser mantida em segredo e não precisa ser compartilhada com ninguém, diminuindo o risco de furto da informação.

Posto isso, vamos para o funcionamento do método RSA em si. O primeiro passo para codificar usando esse método consiste em transformar a mensagem em uma sequência de números, tomando como base a tabela ASCII, mostrada abaixo. Essa tabela é

facilmente encontrada na internet e pode possuir algumas variações. Como o termo ASCII significa "American Standard Code for Information Interchang", os termos na tabela geralmente aparecem em inglês.

Figura 6 – Tabela ASCII

ASCII control characters			ASCII printable characters					
00	NULL	(Null character)	32	space	64	@	96	`
01	SOH	(Start of Header)	33	!	65	A	97	a
02	STX	(Start of Text)	34	"	66	B	98	b
03	ETX	(End of Text)	35	#	67	C	99	c
04	EOT	(End of Trans.)	36	$	68	D	100	d
05	ENQ	(Enquiry)	37	%	69	E	101	e
06	ACK	(Acknowledgement)	38	&	70	F	102	f
07	BEL	(Bell)	39	'	71	G	103	g
08	BS	(Backspace)	40	(	72	H	104	h
09	HT	(Horizontal Tab)	41	)	73	I	105	i
10	LF	(Line feed)	42	*	74	J	106	j
11	VT	(Vertical Tab)	43	+	75	K	107	k
12	FF	(Form feed)	44	,	76	L	108	l
13	CR	(Carriage return)	45	-	77	M	109	m
14	SO	(Shift Out)	46	.	78	N	110	n
15	SI	(Shift In)	47	/	79	O	111	o
16	DLE	(Data link escape)	48	0	80	P	112	p
17	DC1	(Device control 1)	49	1	81	Q	113	q
18	DC2	(Device control 2)	50	2	82	R	114	r
19	DC3	(Device control 3)	51	3	83	S	115	s
20	DC4	(Device control 4)	52	4	84	T	116	t
21	NAK	(Negative acknowl.)	53	5	85	U	117	u
22	SYN	(Synchronous idle)	54	6	86	V	118	v
23	ETB	(End of trans. block)	55	7	87	W	119	w
24	CAN	(Cancel)	56	8	88	X	120	x
25	EM	(End of medium)	57	9	89	Y	121	y
26	SUB	(Substitute)	58	:	90	Z	122	z
27	ESC	(Escape)	59	;	91	[	123	{
28	FS	(File separator)	60	<	92	\	124	|
29	GS	(Group separator)	61	=	93	]	125	}
30	RS	(Record separator)	62	>	94	^	126	~
31	US	(Unit separator)	63	?	95	_		
127	DEL	(Delete)						

Fonte: TreinaWeb, 2019

Em posse da tabela ASCII, trocamos cada letra da mensagem pelo número correspondente na tabela. A título de exemplo, vamos usar a mensagem "RSA". Pela tabela ASCII, então, nossa mensagem passaria a ser a sequência 828365. Como segundo passo, dividimos nossa sequência em blocos menores de números - denotaremos esses blocos pela letra b. Cada bloco desse deverá ter tamanho menor que a chave pública. É importante também tomar o cuidado de se escolher blocos que não tenham correspondência com nenhum elemento linguístico, como letras e palavras, a fim de evitar a criptoanálise sistemática, mencionada no capítulo segundo. Tomemos, no nosso exemplo, os blocos 82-83-65.

Depois disso, escolhe-se dois números primos p e q de tal forma em que se calculará um terceiro número $n = pq$. Esse número n é nossa chave pública, ou seja, a chave de codificação que está aberta para todos verem. Escolheremos, para nosso exemplo, os números primos 11 e 17 e, portanto, a chave pública será igual a 187.

Com isso, conclui-se a pré codificação e podemos passar à codificação.

6.3 Codificação e decodificação

Para codificarmos a mensagem, precisaremos da chave pública n e de um inteiro k que seja inversível módulo $\phi(n)$, o que significa que $\phi(n)$ e k são primos entre si - ou seja, o $mdc(k, \phi(n)) = 1$. No próximo tópico, explicaremos como escolher os números p, q e k de forma a garantir que o método dará certo. Dependendo dos números escolhidos, podemos impossibilitar a decodificação de nossa mensagem no futuro.

Em posse desses números, codificaremos cada bloco de nossa mensagem por vez, da seguinte maneira: calcularemos $b^k \equiv a \pmod{n}$, sendo a cada bloco da mensagem codificada. No caso em que estamos trabalhando, escolheremos o k como sendo 3 e, portanto, calculamos 3 números:

- $82^3 \equiv 92 \pmod{187}$
- $83^3 \equiv 128 \pmod{187}$
- $65^3 \equiv 109 \pmod{187}$

Assim, nossos blocos 82-83-65 foram codificados nos blocos 92-128-109. Como, então, o destinatário da mensagem poderia ter acesso à mensagem original?

Para decodificar essa mensagem, precisaremos da chave privada - chave essa que só quem a possui é o destinatário da mensagem. Para sabermos quem é a chave privada, precisamos de dois números, sendo que um deles é o n, a chave pública, e o outro será denotado como d e calculado da seguinte maneira: $kd \equiv 1 \pmod{(p-1).(q-1)}$. Ou seja, o número d será o inverso de $k \pmod{(p-1).(q-1)}$. Para visualizarmos melhor, voltemos ao nosso exemplo. Como $k = 3$, então $3d \equiv 1 \pmod{160}$. Achamos, portanto, $d = 107$.

Tendo em mãos o elemento d, podemos passar à fase de decodificação. Para decodificar a mensagem precisamos fazer o seguinte cálculo: $a^d \equiv b \pmod{n}$ e, assim, voltaremos cada bloco codificado para cada bloco inicial b, retornando a mensagem original.

Fazendo esses cálculos para nossa mensagem codificada, encontramos o seguinte:

- $92^{107} \equiv 82 \pmod{187}$
- $128^{107} \equiv 83 \pmod{187}$
- $109^{107} \equiv 65 \pmod{187}$

Ou seja, temos a mensagem decodificada nos blocos 82-83-65, o que nos retorna a mensagem inicial “RSA”, pela tabela ASCII.

Com isso, entendemos como criptografar e descriptografar usando método RSA na prática. Porém, podemos nos perguntar se esse método funciona para qualquer valor

escolhido e o porquê de ser um método altamente seguro. Começaremos respondendo a primeira dessas perguntas.

6.4 Escolhendo p, q e k

Primeiramente, podemos observar que o número k não pode ser par, por um simples motivo: escolhidos p e q números primos grandes, certamente são números ímpares e, portanto, $(p-1)$ e $(q-1)$ são números pares. Logo, o resultado do produto de $(p-1)$ por $(q-1)$ será um número par. Encolhendo k como também um número par, não existirá o inverso de k módulo $(p-1)(q-1)$, o que impossibilitará a decodificação de nossa mensagem. Portanto, chegamos à conclusão que o número escolhido k deve ser ímpar. Ainda assim, porém, podemos recair no mesmo problema.

Voltemos ao exemplo que fizemos. Se, ao invés de escolher p e q como os números 7 e 11, tivéssemos os escolhido como 5 e 7, então o produto $(p-1)(q-1)$ seria igual a 24. E sendo 24 um número múltiplo de 3 (valor de nosso k), não existiria, também nesse caso, o inverso de 3 módulo 24. O que podemos fazer então para garantir que dará certo?

Para começar, uniformizaremos o valor de k. A partir disso, podemos construir hipóteses para a criação dos primos p e q para garantir que o inverso sempre exista. De modo geral, usa-se o valor de $k = 3$, como fizemos em nosso exemplo.

Partindo desse valor para k, vamos pensar nos primos p e q de forma que ambos sejam congruentes à 5 módulo 6. Isso garantirá que sempre teremos 3 inversível módulo $((p-1)(q-1))$. Por quê? Entenderemos abaixo.

Se $p \equiv 5 \pmod 6$, então $p-1 \equiv 4 \pmod 6$. De modo análogo, $q-1 \equiv 4 \pmod 6$. Multiplicaremos então, as duas congruências, ficando com:

$$(p-1)(q-1) \equiv 16 \equiv 4 \pmod 6$$

Portanto,

$$(p-1)(q-1) = 6h + 4 = 6h + 3 + 1 \qquad , h \in \mathbb{Z}$$

Fatorando o segundo membro, temos:

$$(p-1)(q-1) = 3(2h+1) + 1$$

Depois, isolamos o termo $3(2h+1)$ e ficamos com

$$3(2h+1) = (p-1)(q-1) - 1$$

Substituindo $(p-1)(q-1)$ por $(6h+4)$, nossa equação fica assim:

$$3(2h+1) = (6h+4) - 1$$

Temos então uma nova congruência,

$$3(2h+1) \equiv -1 \pmod{6h+4}$$

Podemos multiplicar por -1 ambos os lados e teremos

$$3(-2h-1) \equiv 1 \pmod{6h+4}$$

E como

$$(-2h-1) \equiv (4h+3) \pmod{6h+4}$$

Então

$$3(4h+3) \equiv 1 \pmod{6h+4}.$$

E obtemos o resultado esperado.

Esse algoritmo não só nos garante a existência do inverso, mas também nos dá uma formula para calculá-lo - basta ver que $(4h+3) = d$.

Veremos agora uma breve demonstração do porque o método RSA realmente funciona.

6.5 Prova da funcionalidade do método RSA

O que queremos provar é que ao decodificarmos cada bloco a de nossa mensagem codificada, retornamos aos respectivos blocos b de nossa mensagem original.

Começaremos relembrando que os blocos da mensagem codificada têm que ser maiores ou iguais à 1 e menores que n, ou seja, $1 \leq b < n$.

Peguemos a fórmula para codificar cada bloco, $b^k \equiv a \pmod{n}$, e tomemos nosso a no intervalo $0 \leq a < n$. Depois, relembremos a formula para decodificação, $a^d \equiv r \pmod{n}$, tomando nosso r no mesmo intervalo de a, ou seja, $0 \leq r < n$.

Agora, o que queremos mostrar é que $r = b$. Caso não seja verdade, o método de nada serve, já que a mensagem decodificada seria diferente da mensagem original.

Uma coisa importante a ser notada é que, como $r \equiv a^d \pmod{n}$ e $a \equiv b^k \pmod{n}$, então $r \equiv b^{kd} \pmod{n}$ (1). Guardemos esse resultado, que será importante mais à frente.

Já vimos nesse capítulo que a chave privada d é calculada como $kd \equiv 1 \pmod{(p-1).(q-1)}$, o que significa que $kd = 1 + s(p-1)(q-1)$, sendo s um inteiro qualquer. Substituindo esse resultado em (1), ficamos com:

$$r \equiv b^{1+s(p-1)(q-1)} \pmod{n} \equiv b^{s(p-1)(q-1)}b \pmod{n} \qquad (2)$$

Nosso objetivo, chegado esse ponto da demonstração, é provar que $b^{kd} \equiv b \pmod{n}$. Dividiremos essa demonstração em dois casos:

1. Caso o $mdc(p, b) \neq 1$, como p é um número primo, então obrigatoriamente b é múltiplo de p. Então $b = xp$, sendo $x \in \mathbb{Z}$. Daí, temos que:

$$\begin{aligned} b &\equiv 0 \pmod{p} \\ \Rightarrow b^{kd} &\equiv 0 \pmod{p} \\ \Rightarrow b^{kd} &\equiv b \pmod{p}. \end{aligned}$$

2. Caso o $mdc(p, b) = 1$, tomaremos outro caminho. Reescreveremos (2) como sendo:

$$b^{kd} \equiv b^{(p-1)s(q-1)}b \pmod{p}.$$

   Graças ao Teorema de Fermat, podemos garantir que o número $b^{(p-1)} \equiv 1 \pmod{p}$. Então,

$$\begin{aligned} b^{kd} &\equiv 1^{s(q-1)}b \pmod{p} \\ \Rightarrow b^{kd} &\equiv b \pmod{p}. \end{aligned}$$

Repetindo exatamente as mesmas passagens, usando o número primo q no lugar de p, concluímos também que $b^{kd} \equiv b \pmod{q}$.

Portanto, b^{kd} é simultaneamente congruente à b módulo p e módulo q. Isso significa que $b^{kd} = t_1p + b$ e $b^{kd} = t_2q + b$, com t_1 e t_2 sendo dois inteiros quaisquer. Ou seja,

1. $b^{kd} - b = t_1p$
2. $b^{kd} - b = t_2p$

Assim, $(b^{kd} - b)$ é um múltiplo de q e de p, ao mesmo tempo. E sendo p e q números primos, $(b^{kd} - b)$ é também um múltiplo do produto pq, ou seja,

$$(b^{kd} - b) = t_3pq, \qquad t_3 \in \mathbb{Z}$$

Daí, temos que:

$$b^{kd} \equiv b \pmod{pq}$$

E, como sabemos, o produto pq nós dá nossa chave pública n e, portanto,

$$b^{kd} \equiv b \pmod{n}$$

Pelo nosso resultado (1), temos então que

$$r \equiv b \pmod{n}$$

O fato de r e b serem equivalentes módulo n não significa, necessariamente, que são iguais. Entretanto, como $1 \leq b < n$ e $0 \leq r < n$, então essa congruência implica a igualdade. Concluímos, por fim, que $r = b$, ou seja, que ao decodificarmos cada bloco a obteremos cada bloco b da mensagem original.

6.6 Porque o RSA é seguro

Pelo exemplo que usamos para codificação e decodificação, o método parece fácil de ser quebrado. Porém, vale ressaltar que foram usados os números primos p e q pequenos de forma a ficar mais didático o exemplo e é exatamente nisso que consiste a solidez do método RSA: utiliza-se números primos que tenham por volta de 200 algarismos, ou seja, números primos grandes, o que torna muito difícil a fatoração da chave pública n. Sem saber quem é a chave pública n, não tem como descobrir nosso elemento d e, portanto, torna-se muito difícil decodificar qualquer mensagem codificada por esse método - esse é um processo que dura meses ou até anos, mesmo com o auxílio de computadores muito potentes.

Segundo Framilson Carneiro, em seu livro "Criptografia e Teoria dos Números",

> Até o momento, não se conhece nenhum algoritmo para a fatoração de inteiros suficientemente grandes em um computador clássico que funcione em tempo polinomial, mas também não se provou que um algoritmo deste tipo não pode existir. Portanto, para as chaves suficientemente grandes, o RSA é seguro, dado o conhecimento matemático atual em relação ao problema da fatoração de inteiros grandes.(CARNEIRO, 2017)

Além disso, o autor estima o tempo necessário e a quantidade de operações que um computador precisaria fazer para fatorar um número, tendo como base sua quantidade de dígitos. Para um número de 200 dígitos, um computador faria cerca de $1{,}2.10^{23}$ operações e demoraria por volta de $3{,}8.10^{9}$ anos para concluir essa fatoração.

Outro fator que contribui para a segurança do método RSA, como já dissemos, é a dificuldade de se encontrar números primos muito grandes. Apesar de não existir uma

fórmula ou algoritmo a ser seguido que sirvam para encontrar novos números primos, existem alguns testes que podem ajudar nesse processo. Os testes de primalidade nos ajudam a testar se um dado número é primo e, mesmo sendo úteis em vários momentos, esses testes possuem suas limitações, como veremos agora.

Primeiramente, consideremos o resultado do teorema abaixo, que nos ajudará a provar o primeiro dos testes. Esse teorema não será demonstrado, uma vez que sua demonstração envolve conceitos que fogem do foco deste trabalho.

Teorema 6.6.1 (**Tchebychef**)**.** *Para $2 \leq m \in \mathbb{N}$, sempre existe um $p \in \mathbb{P}$ tal que $m < p < 2m$.*

Proposição 10. *Para o e-nésimo número primo p_n vale a estimativa*

$$p_n \leq 2^n.$$

Demonstração. Faremos a demonstração por indução. Para $n = 1$, temos $2 = p_1 \leq 2^1$. Por 6.2.1, temos que $p_n < p_{n+1} < 2p_n$. De $p_n \leq 2^n$ segue que $p_{n+1} \leq 2 \cdot 2^n = 2^{n+1}$. □

Existe ainda outro método utilizado como teste para números pequenos e é base para o que chamamos de Crivo de Erastótenes:

Teorema 6.6.2. *Seja $1 < n \in \mathbb{N}$. Se n não é divisível por nenhum $p \in \mathbb{P}$, tal que $p \leq \sqrt{n}$, então n é primo.*

Por exemplo, escolhemos $n = 100$. Nesse caso, os números primos menores ou iguais a $\sqrt{100} = 10$ são: 2, 3, 5 e 7. Como 2 e 5 dividem 10, então 100 não é primo.

Exemplo 2: Para $n = 19$, temos que $\sqrt{19} \approx 4,35$. Os números primos menores ou iguais a 4 são os números 2 e 3. Como nem 2 e nem 3 dividem 19, 19 é primo.

Demonstração. Seja $n > 1$ e p um número primo tal que $p \nmid n$ e $p \leq \sqrt{n}$.

Suponhamos, por absurdo, que n não é primo. Seja $q \in \mathbb{P}$ o menor divisor de n, ou seja, $n = q \cdot k$, $q \leq k$ e $k \in \mathbb{Z}$. Daí, temos então:

$$q \leq k$$
$$\Rightarrow q \cdot q \leq k \cdot q$$
$$\Rightarrow q^2 \leq n$$

Ou seja, n é divisível por q, o que é uma contradição. □

A partir desse resultado, podemos entender o Crivo de Erastótenes. Esse crivo é um algoritmo que nos permite descobrir quantos e quais números primos existem até um determinado número $n \in \mathbb{N}$ tal que $2 \leq n$.

Para isso, escreve-se todos os números inteiros positivos até n. Depois, risca-se todos os números pares maiores que 2 e menores que n. Como passo seguinte, risca-se todos os múltiplos de 3, maiores que 3. Seguimos esses passos, riscando os múltiplos dos próximos números primos, até que sobrem somente números primos entre 2 e n. Vemos que basta riscar os os múltiplos de todos os primos até o maior primo $p \leq n$.

Como exemplo, faremos para $n = 100$: Riscando, na lista $\{2, 3, 4, 5, ..., 100\}$, os múltiplos dos números primos até 7 (ja que 7 é o maior primo $p \leq n$), sobram apenas os 25 primos $\{2, 3, 5, 7, ..., 97\}$.

Note que esse método é falho para números muito grandes, considerando o trabalho mecânico para desconsiderar os múltiplos de todos os primos até o maior primo $p \leq n$, se n é muito grande.

Podemos ainda ter uma outra abordagem, como segue abaixo:

Teorema 6.6.3. *Seja $n \in \mathbb{N}$ ímpar, então entre os pares de inteiros (x, y) com*

$$0 \leq y < x \leq n = x^2 - y^2$$

e os pares (r, s) tais que

$$1 \leq s \leq r \leq n = rs$$

existe uma correspondência biunívoca natural.

Demonstração. Se $n = x^2 - y^2$, com $0 \leq y < x \leq n$, basta escolhermos $r = x + y$ e $s = x - y$ e segue que $n = rs$ e $1 \leq s \leq r \leq n$.

Reciprocamente, seja $n = rs$ com $1 \leq s \leq r \leq n$. Como n é ímpar, então r e s são ímpares e $\frac{r+s}{2}$ e $\frac{r-s}{2}$ são inteiros. Peguemos $x = \frac{r+s}{2}$ e $y = \frac{r-s}{2}$. Temos então $x, y \in \mathbb{N}_0$ e $0 \leq y;, x \leq n$. Além disso, vale

$$x^2 - y^2 = \frac{(r+s)^2 - (r-s)^2}{4} = rs = n.$$

□

Como consequência desse teorema, temos o seguinte corolário.

Corolário 6.6.3.1. *Seja $n \in \mathbb{N}$ ímpar, então*

1. *n possui tantas decomposições distintas $n = x^2 - y^2$ como diferença de dois quadrados quantas decomposições multiplicativas distintas $n = rs$ ele admite.*

2. *n é um número primo se, e somente se*

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$$

é a única decomposição de n como diferença de dois quadrados.

Como exemplo, tomemos $n = 33 = 33 \cdot 1 = 11 \cdot 3$ temos

$$33 = 17^2 - 16^2 = 7^2 - 4^2.$$

Em geral, para $n = pq = pq \cdot 1 = p \cdot q$, onde $q \leq p$ são primos, temos as decomposições correspondentes como diferença de dois quadrados:

$$n = pq = \left(\frac{pq+1}{2}\right)^2 - \left(\frac{pq-1}{2}\right)^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$

Para um segundo exemplo, tomemos $n = 9 = 9 \cdot 1 = 3 \cdot 3$ e teremos

$$9 = 5^2 - 4^2 = 3^2 - 0^2.$$

A decomposição de um número ímpar n como diferença de dois quadrados pode ser favorável quando $n = rs$ com $y = r - s$ "pequeno". Isso pode servir para descobrir a decomposição primária de um tal número. Abaixo, segue um exemplo para demosntrar essa ideia.

Vamos tentar descobrir se $n = 2438323$ é um número primo ou não. Se tentarmos usar o Crivo de Eratóstenes, teremos $\sqrt{n} \approx 1561,51$ e as tentativas de tentar descobrir se esse n é divisível por algum primo $p \leq 1561$ são decepcionantes.

Porém, escrevendo-se $y^2 = x^2 - n$, começando com $x = 1562$, vemos que $x^2 - n$ é de fato um quadrado perfeito y^2 com $y = 39$. Isto nos dá a decomposição $n = (1562 + 39)(1562 - 39) = 1601 \cdot 1523$. Esta é a decomposição completa de n, pois 1523 e 1601 são realmente primos (senão n já teria sido divisível por algum $p \leq 37$).

É interessante notar que se $n = p(p+2)$ é, por exemplo, o produto de dois primos gêmeos (sem que se saiba previamente disso), esse método, observando-se $p < \sqrt{n} = \sqrt{p(p+2)} < \sqrt{p^2 + 2p + 1} = p + 1$, fornece logo no primeiro passo, para $x = p + 1$:

$$(p+1)^2 - n = (p+1)^2 - p(p+2) = 1^2,$$

ou seja, decomposição $n = [(p+1) + 1] \cdot [(p+1) - 1]$.

Com isso, pode-se perceber que encontrar números primos grande é, de fato, uma tarefa difícil e que, portanto, o método de criptografia RSA, por se basear nessa dificuldade, é um método muito seguro.

Considerações Finais

O estudo da criptografia, com enfoque no método de criptografia RSA, faz com que fiquemos menos alheios à realidade que nos cerca, permitindo-nos entender os detalhes de processos tão presentes em nosso dia a dia. Além disso, permite que se crie um campo fértil de desenvolvimento do pensamento computacional - recurso tão necessário para o ensino da matemática na formação de professores, em concomitância com a resolução de problemas.

Considerando a metodologia utilizada neste trabalho, pesquisa bibliográfica, acreditamos ter atingido o objetivo de mostrar como o estudo do método de criptografia RSA pode ser útil no desenvolvimento do pensamento computacional. Ao se estudar o processo de desenvolvimento histórico desse tema, as bases da Teoria dos números que o fundamentam e cada parte do processo do método de criptografia RSA, trabalham-se fluxogramas e algoritmos, técnicas de resolução de problemas e conceitos lógicos matemáticos e, portanto, desenvolve-se o pensamento computacional, paralelamente a cada conteúdo deste trabalho.

Referências

ADÃO, P. *Números, cirurgias e nós de gravata*. Lisboa: Instituto Superior Técnico, 2012.

BARBOSA, H. F. *Teoria dos Números e Criptografia*. Monografia — Universidade Federal de São Carlos, São Carlos, 2008.

BES, P. et al. *Metodologias para aprendizagem ativa*. Porto Alegre: Grupo A, 2019.

BRASIL. *Ministério da Educação*. [S.l.]: Base Nacional Comum Curricular. Brasilia, 2018.

BURNETT, S. *Criptografia e segurança: o guia oficial RSA*. [S.l.]: Gulf Professional Publishing, 2002.

CAMPELLO, A. C.; LEAL, I. *Teoria Aritmética dos Números e Criptografia RSA*. Monografia — Universidade Estadual de Campinas, 2007.

CARNEIRO, F. J. F. *Criptografia e Teoria dos Números*. Rio de Janeiro: Ciência Moderna, 2017.

CASTRO, F. L. *Criptografia RSA: Uma abordagem para os professores do ensino básico*. Monografia — Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

CIMINO, A. *A história da quebra dos códigos secretos*. São Paulo: M.Books, 2018. v. 1.

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

COUTINHO, S. C. *Teoria dos Números e Criptografia*. [S.l.]: Associação Instituto Nacional de Matemática Pura e Aplicada - IMPA, 2015.

D'AMBROSIO, B. s. Como ensinar matemática hoje? *SBEM*, 1989.

DIESEL, A.; BALDEZ, A. L. S.; MARTINS, S. N. Os princípios das metodologias ativas de ensino: uma abordagem teórica. *Revista Thema*, v. 14, n. 1, p. 268–288, 2017.

ECHEVERIA, M. d. P. P.; POZO, J. I. Aprender a resolver problemas e resolver problemas para aprender. *Universidade autônoma de Madrid*, 1988.

FERNANDES, S. H. et al. *Novas trajetórias de formação - Matemática*. São Paulo: FTD, 2021.

FIARRESGA, V. M. C. et al. *Criptografia e matemática*. Tese (Doutorado), 2010.

FILATRO, C. C. C. A. *Metodologias Inov-ativas na educação presencial, a distância e corporativa*. São Paulo: Saraiva, 2018.

FREITAS, L. M. T. D. et al. *Novas práticas para o ensino médio*. [S.l.]: Editora do Brasil, 2020.

LIBÂNEO, J. C. *Adeus professor, adeus professora? novas exigências educacionais e profissão docente*. [S.l.]: Cortez, 1998.

LOVATO, F. L.; MICHELOTTI, A.; LORETO, E. L. da S. Metodologias ativas de aprendizagem: uma breve revisão. *Acta Scientiae*, v. 20, n. 2, 2018.

LUCKESI, C. C. *Avaliação da aprendizagem escolar*. [S.l.]: Cortez, 2002.

MAX, F. *Storytelling e suas aplicações no mundo dos negócios*. [S.l.]: Grupo GEN, 2015.

MORÁN, J. Mudando a educação com metodologias ativas. *Coleção mídias contemporâneas. Convergências midiáticas, educação e cidadania: aproximações jovens*, v. 2, n. 1, p. 15–33, 2015.

NETO, J. L. de M. Teoria dos números e criptografia. 2005.

NOGUEIRA, D. R. et al. *Revolucionando a sala de aula 2 - Novas metodologias ainda mais ativas*. Rio de Janeiro: Grupo GEN, 2020.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. *Segurança Digital [Revista online]*, v. 31, p. 11–15, 2012.

ONUCHIC, L. d. l. R. *Resolução de problemas: teoria e prática*. [S.l.]: Paco Editorial, 2019.

PAIVA, M. R. F. et al. Metodologias ativas de ensino-aprendizagem: revisão integrativa. *SANARE-Revista de Políticas Públicas*, v. 15, n. 2, 2016.

POLYA, G. *A arte de resolver problemas: um novo aspecto do método matemático*. Rio de Janeiro: Interciência Ltda., 1995.

PONTE, J. P. da; BROCARDO, J.; OLIVEIRA, H. *Investigações matemáticas na sala de aula*. São Paulo: Grupo Autêntica, 2007.

ROMANATTO, M. C. Resolução de problemas nas aulas de matemática. *Revista Eletrônica de Educação*, v. 6, n. 1, p. 299–311, 2012.

SANTOS, M. d. s. dos et al. *Pensamento computacional*. Porto Alegre: Grupo A, 2021.

SILVA, W. W. de M. *A evolução da criptografia e suas técnicas ao longo da história*. Monografia — Instituto Federal de Goiania, 2019.

SOUZA, A. S. D.; OLIVEIRA, G. S. D.; ALVES, L. H. A pesquisa bibliográfica: Principios e fundamentos. *Cadernos da Fucamp*, v. 20, n. 43, 2021.

VICENTE, A. et al. A criptografia e sua importÂncia na atualidade. *Revista Aten@*, v. 1, n. 0, 2016.

ZOELNER, É. G. et al. Criptografia. *Anais do EVINCI-UniBrasil*, v. 3, n. 1, p. 333–333, 2017.

Documento Digitalizado Público

TCC GUILHERME GUIMARÃES

Assunto: TCC GUILHERME GUIMARÃES
Assinado por: Antonio Neto
Tipo do Documento: Trabalho de Conclusão de Curso - TCC
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original

Documento assinado eletronicamente por:

- **Antonio Dantas Costa Neto**, **COORDENADOR DE CURSO - FUC1 - ES-GRAD-LM**, em 31/01/2023 15:43:12.

Este documento foi armazenado no SUAP em 31/01/2023. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 427513
Código de Autenticação: 3ae26bd959