Impactos da demonstração da Conjectura Forte de Goldbach nos sistemas criptográficos modernos

Joel Lucas Barros de Oliveira

Mossoró, 2025

INTRODUÇÃO/JUSTIFICATIVA

Atualmente, estamos vivendo a chamada Era da Informação, um período caracterizado por uma explosão no volume de dados gerados, processados e armazenados em plataformas digitais. Nesse contexto, informações tornaram-se a principal mercadoria do mundo contemporâneo, sendo alvo de interesse de indivíduos, empresas privadas, instituições públicas e governos. O domínio e a proteção desses dados determinam não apenas a vantagem competitiva de corporações, mas também a estabilidade econômica, a soberania nacional e a privacidade individual. Portanto, a segurança da informação emergiu como uma das grandes preocupações do nosso tempo, o que torna a discussão sobre criptografia extremamente pertinente e atual.

A criptografia, nesse cenário, apresenta-se como uma das ferramentas mais importantes para assegurar que comunicações e dados permaneçam protegidos contra acessos não autorizados. Ela tem como princípio fundamental garantir que a comunicação entre remetente e destinatário ocorra de maneira sigilosa, impedindo que terceiros tenham acesso ao conteúdo compartilhado (Ludwig et al., 2020). A aplicação da criptografia vai desde o uso pessoal em aplicativos de mensagens até sistemas bancários, operações militares e tecnologias críticas para infraestruturas nacionais. Para fazer cumprir esse princípio de confidencialidade e integridade, os algoritmos criptográficos modernos se baseiam em construções matemáticas complexas, muitas delas centradas em propriedades dos números primos e em dificuldades computacionais associadas a esses números.

Um dos algoritmos mais conhecidos e utilizados mundialmente é a cifra RSA, criada por Ron Rivest, Adi Shamir e Leonard Adleman - a sigla RSA é derivada das iniciais de seus criadores. Esse algoritmo assimétrico estabelece um par de chaves — uma pública e uma privada — ligadas por uma operação matemática que permite a encriptação e posterior desencriptação da informação. O funcionamento do RSA depende da geração de um número n, produto de dois primos grandes, p′ e p″, cada um com cerca de 100 algarismos. Embora o número nnn possa ser divulgado livremente, a segurança do sistema depende da enorme dificuldade de se fatorar esse número em seus fatores primos, o que se presume ser praticamente impossível com os recursos computacionais atuais (Patil et al., 2016, apud Ludwig et al., 2020).

A criptografia RSA, portanto, sustenta-se sobre uma suposição: fatorar um número grande em seus componentes primos é computacionalmente inviável. No entanto, como toda suposição científica, ela está sujeita a revisão à luz de novos conhecimentos. É nesse ponto que o presente trabalho de pesquisa se insere. O objetivo é investigar possíveis interseções entre a criptografia moderna baseada em primos e um dos maiores enigmas ainda não resolvidos da Teoria dos Números: a Conjectura Forte de Goldbach.

A Conjectura Forte de Goldbach, proposta em 1742, afirma que "todo número par maior que 2 pode ser escrito como a soma de dois números primos". A beleza dessa conjectura reside justamente em sua simplicidade de enunciado e profundidade de implicações. Apesar dos esforços de gerações de matemáticos, a conjectura permanece sem uma demonstração formal e completa, embora tenham sido obtidos importantes resultados intermediários, como os de Hardy e Littlewood, Vinogradov e, em especial, Chen Jingrun. Este último demonstrou que todo número par suficientemente grande pode ser expresso como a soma de um número primo e de um produto de, no máximo, dois primos — o chamado "primo quase-primo", resultado hoje conhecido como Teorema de Chen (PAIVA et al., 2024).

Esses avanços parciais podem, à primeira vista, parecer estritamente teóricos, limitados ao campo da matemática pura. No entanto, a matemática moderna — especialmente a Teoria dos Números — tem provado, de forma recorrente, que descobertas puramente abstratas podem ter aplicações concretas e transformadoras em áreas como segurança cibernética, física quântica, engenharia de comunicações e ciência de dados. Assim, a motivação principal deste trabalho é explorar se há ou pode haver conexões entre os avanços rumo à prova da Conjectura de Goldbach e possíveis vulnerabilidades nas cifras que fundamentam a segurança digital contemporânea.

A justificativa para essa linha de investigação repousa sobre dois pilares principais. O primeiro é de ordem epistemológica e científica: a pesquisa avança no sentido de conectar dois campos que, embora intimamente ligados pela matemática, raramente são abordados juntos — a criptografia prática e a Teoria dos Números em seu estado mais puro. O segundo pilar é de relevância social e tecnológica: vivemos uma era em que nossas finanças, comunicações, identidades e dados de saúde são transmitidos digitalmente. Qualquer avanço que comprometa os alicerces teóricos da criptografia tradicional terá impacto direto e imediato na sociedade.

Especificamente, o trabalho parte da seguinte hipótese: se forem obtidos avanços teóricos substanciais na compreensão da estrutura e distribuição dos números primos — como uma eventual demonstração da Conjectura de Goldbach ou resultados próximos a ela —, essas descobertas podem revelar padrões ou propriedades até então desconhecidos, que impactam diretamente a premissa de segurança dos algoritmos criptográficos baseados na dificuldade da fatoração de inteiros. Isso não seria uma novidade, pois ao longo da história diversos algoritmos de encriptação foram quebrados após avanços da matemática pura. Como exemplo pode-se citar a Cifra de César, que foi decifrada após avanços em estudos de probabilidade e distribuição de frequência, e o Código Enigma, usado pela Alemanha Nazista durante a Segunda Guerra Mundial, que foi quebrado após avanços feitos nas áreas de computação de grandes números.

Além disso, o próprio exercício de refletir sobre essa hipótese obriga-nos a repensar os fundamentos dos algoritmos criptográficos em uso. Muitos deles dependem não apenas da fatoração de inteiros, mas também de problemas matemáticos difíceis e não resolvidos — como logaritmos discretos e curvas elípticas. Isso revela que a segurança digital está, em parte, sustentada sobre estruturas cuja solidez é probabilística, não absoluta.

Nesse sentido, a pesquisa que se propõe aqui é também um chamado à prudência e ao preparo tecnológico. Mesmo que a demonstração da Conjectura de Goldbach ainda esteja distante, o simples fato de que os resultados parciais — como o de Chen — tenham evoluído mostra que o campo avança. Esse avanço pode, a qualquer momento, trazer à tona relações inesperadas entre primos que comprometam a aleatoriedade ou a imprevisibilidade que os algoritmos modernos presumem como garantida. Como exemplo, podemos citar o recente crescimento do campo da criptografia quântica e pós-quântica, que já busca antecipar os impactos que computadores quânticos podem trazer ao quebrar sistemas clássicos como RSA e ECC (criptografia de curvas elípticas).

Portanto, a relevância da pesquisa também reside na antecipação de riscos e na proposição de alternativas viáveis. Se confirmada alguma relação entre resultados da Teoria dos Números e fragilidades criptográficas, será necessário desenvolver novos algoritmos baseados em problemas ainda mais robustos — como aqueles derivados de redes vetoriais (lattices), isogenias de curvas elípticas, problemas combinatórios não estruturados, ou logaritmos discretos em grupos não

convencionais. O trabalho, portanto, não se limita à crítica ou análise dos sistemas existentes, mas pretende contribuir ativamente para a busca de soluções mais seguras, duradouras e resistentes.

Outro aspecto importante é o caráter interdisciplinar da pesquisa. A articulação entre matemática pura e aplicada, ciência da computação, engenharia de dados e cibersegurança exige do pesquisador uma formação abrangente, que transite entre abstrações teóricas profundas e ferramentas computacionais avançadas. Ao propor esse diálogo entre áreas, o trabalho também pretende contribuir para uma formação acadêmica mais integrada, capaz de responder aos desafios complexos da atualidade com soluções igualmente complexas e bem fundamentadas.

Finalmente, é preciso destacar o papel ético e social da investigação. Ao lidar com segurança da informação, privacidade digital e proteção de dados sensíveis, o pesquisador deve estar consciente da responsabilidade que carrega. A criptografia, mais do que uma ferramenta técnica, é hoje um direito civil, essencial para o exercício da liberdade individual, da segurança jurídica e da autodeterminação informacional. Qualquer descoberta que ponha em risco os mecanismos que garantem esse direito deve ser tratada com seriedade, transparência e espírito de colaboração científica.

Em suma, esta introdução e justificativa visam apresentar a base lógica, científica e social da pesquisa proposta. Partindo da relação entre a Conjectura Forte de Goldbach e os sistemas criptográficos modernos, especialmente a cifra RSA, busca-se investigar como avanços na Teoria dos Números podem afetar diretamente a segurança digital da sociedade contemporânea. Ao integrar revisão teórica, reflexão crítica e proposição de soluções, o trabalho pretende contribuir para o avanço do conhecimento em um campo estratégico para o futuro da informação, da tecnologia e da própria democracia digital.

OBJETIVOS

GERAL: Investigar as potenciais consequências para os sistemas criptográficos modernos decorrentes da demonstração da Conjectura Forte de Goldbach.

ESPECÍFICOS:

- "Analisar as vulnerabilidades potenciais do algoritmo RSA e outros sistemas criptográficos baseados em primos, considerando os avanços teóricos relacionados à Conjectura de Goldbach."
- "Mostrar, se preciso e possível, a necessidade de modificação e/ou criação de novos algoritmos de criptografia que escapem das vulnerabilidades que a demonstração da Conjectura Forte de Goldbach possa vir a trazer."
- "Investigar a possibilidade de algoritmos baseados em primos mostrarem novas alternativas na busca da demonstração da Conjectura Forte de Goldbach."

METODOLOGIA

Inicialmente, foi estabelecido o tema de pesquisa e, após isso, definidos os objetivos a serem alcançados com a mesma. Com isso traçado, o próximo passo será realizar uma revisão sistemática da literatura com o intuito de mapear o estado atual do conhecimento sobre tópicos interligados, como criptografia, a Conjectura Forte de Goldbach, propriedades dos números primos e outras estruturas matemáticas associadas. Essa revisão bibliográfica buscará integrar fontes clássicas e contemporâneas, abrangendo artigos científicos, dissertações, teses e livros especializados, tanto nacionais quanto internacionais. Será dada atenção especial a publicações que tratem dos fundamentos teóricos da criptografia moderna e das tentativas parciais de prova da conjectura de Goldbach, mesmo que esses temas sejam abordados de forma independente.

Essa etapa é fundamental para embasar teoricamente a pesquisa, delimitar os campos de atuação e identificar lacunas no conhecimento que justifiquem e orientem o aprofundamento da investigação. A busca será feita em bases de dados acadêmicas como Scopus, IEEE Xplore, Google Scholar, JSTOR e SciELO, utilizando palavras-chave como "Goldbach strong conjecture", "cryptography", "prime numbers in encryption", "Chen's theorem", "RSA vulnerabilities", entre outras.

Concluída essa revisão, será realizada uma investigação aprofundada de como os resultados intermediários alcançados nas tentativas de prova da Conjectura Forte de Goldbach — com destaque para o teorema de Chen Jingrun (1933–1996) — podem se relacionar com a robustez e segurança de cifras modernas baseadas em números primos. O resultado de Chen, que demonstra que todo número par suficientemente grande pode ser escrito como a soma de um primo com um número que é o produto de no máximo dois primos, será analisado em termos de suas implicações potenciais para a base matemática dos sistemas de criptografia, em especial a cifra RSA.

O método RSA baseia-se na dificuldade de fatorar o produto de dois primos grandes, o que garante a segurança dos dados criptografados. No entanto, à medida que se aprofundam os estudos sobre padrões e propriedades dos números primos — como ocorre nas pesquisas ligadas à Conjectura de Goldbach — levanta-se a hipótese de que novos resultados podem enfraquecer a suposição de que a fatoração de inteiros é um problema intratável. Assim, serão examinadas as possíveis vulnerabilidades que surgirão caso novas descobertas sobre os primos ou sobre suas combinações viessem a tornar a fatoração mais eficiente ou previsível.

A seguir, a metodologia contempla uma etapa de análise computacional e experimental. Serão desenvolvidos scripts em linguagens como Python ou SageMath para simular e testar comportamentos de sequências numéricas envolvidas na conjectura, bem como suas aplicações em sistemas de criptografia. O objetivo é observar, na prática, possíveis padrões ou irregularidades que possam indicar fragilidades em cifras do tipo RSA ou similares. Também serão estudadas bibliotecas criptográficas conhecidas para compreender como as implementações atuais lidam com os primos e suas propriedades.

Caso se confirme alguma conexão entre as propriedades descritas por Chen Jingrun e a fragilização dos sistemas criptográficos, será iniciada uma nova fase da pesquisa voltada à análise das consequências sociais e tecnológicas dessa vulnerabilidade. Considerando que a segurança da informação é um dos pilares fundamentais da era digital — abrangendo desde comunicações pessoais até sistemas bancários, militares e governamentais — será feita uma reflexão crítica sobre os riscos potenciais que tal descoberta pode representar. Serão analisadas as implicações para a privacidade dos dados, integridade de transações, confiança digital e estrutura da segurança cibernética global.

Diante disso, a pesquisa também se compromete com a proposição de soluções alternativas. Com base no levantamento bibliográfico e nos estudos experimentais, serão exploradas **estratégias criptográficas pós-quânticas**, que não dependem diretamente da dificuldade de fatoração de primos. Algumas dessas soluções promissoras já vêm sendo estudadas na literatura e serão consideradas como potenciais substitutas aos métodos clássicos. Entre elas destacam-se:

- **Problema do Logaritmo Discreto em Grupos Não Convencionais**, que explora a dificuldade de resolver logaritmos em grupos com propriedades específicas;
- **Problema do Lattice (Redes Vetoriais)**, baseado em problemas de aproximação em espaços de alta dimensão, resistentes a ataques quânticos;
- **Problemas com Isogenias de Curvas Elípticas**, que utilizam a estrutura complexa das curvas e suas isogenias para criar sistemas criptográficos robustos;
- **Problemas Combinatórios Não Estruturados**, que evitam padrões regulares e apostam em complexidade computacional intrínseca para garantir segurança.

Essas alternativas serão investigadas não apenas do ponto de vista matemático, mas também quanto à viabilidade de implementação prática, desempenho e aceitação em padrões internacionais de segurança. Espera-se, assim, contribuir com a construção de uma base teórica sólida que sustente futuras aplicações criptográficas mais seguras, mesmo frente aos avanços da matemática e da computação.

Em síntese, esta metodologia articula fundamentação teórica, investigação matemática profunda, simulações computacionais e análise aplicada, de forma a proporcionar uma abordagem completa sobre a relação entre conjecturas matemáticas e segurança digital. Ao final do plano de trabalho, espera-se que o pesquisador esteja apto a compreender criticamente os fundamentos da criptografia e a propor soluções matemáticas viáveis diante de novos desafios emergentes.

HABILIDADES A SEREM DESENVOLVIDAS

Durante o desenvolvimento deste plano de trabalho, espera-se que o pesquisador desenvolva um conjunto de habilidades técnicas e intelectuais que dialoguem tanto com a matemática pura quanto com suas aplicações em áreas como segurança da informação, computação e criptografia. Em primeiro lugar, destaca-se a habilidade de compreender profundamente como os fundamentos da matemática teórica, especialmente da Teoria dos Números, se relacionam com a prática contemporânea, sobretudo no campo da proteção de dados e informações digitais. Essa competência envolve o estudo avançado de estruturas numéricas, como os números primos, e a análise de sua aplicação em algoritmos criptográficos utilizados em escala global, incluindo aqueles empregados em sistemas bancários, redes privadas virtuais e plataformas de comunicação digital segura.

Além disso, o trabalho proporciona a oportunidade de refinar a capacidade de realizar investigações interdisciplinares, transitando entre campos clássicos da matemática e demandas atuais da tecnologia. Desenvolver essa habilidade é essencial para enfrentar problemas complexos que exigem a articulação de múltiplos saberes, como os desafios emergentes da criptografia pós-quântica. O contato com algoritmos criptográficos baseados em problemas matemáticos de difícil resolução, como fatoração de inteiros, logaritmo discreto e estruturas baseadas em lattices, permite ao pesquisador construir uma visão crítica sobre a eficácia e as limitações dessas técnicas, ampliando sua competência analítica e investigativa.

Outro ponto importante diz respeito ao desenvolvimento de uma mentalidade investigativa voltada à revisão de problemas clássicos sob novas perspectivas. Por exemplo, ao estudar algoritmos criptográficos que operam com números primos, o pesquisador é levado a revisitar problemas não resolvidos da Teoria dos Números, como a Conjectura Forte de Goldbach, com o olhar de quem busca padrões, propriedades e possibilidades de aplicação computacional. Isso estimula a habilidade de propor abordagens inovadoras, exercitando a criatividade matemática e a capacidade de formular hipóteses baseadas em observações empíricas geradas por ferramentas computacionais modernas e eficientes.

Adicionalmente, o plano favorece o desenvolvimento de competências em programação matemática e uso de software científico, essenciais para modelar algoritmos, testar conjecturas e simular grandes conjuntos de dados numéricos. Como exemplo de softwares que podem realizar este tipo de atividade podemos citar o Mathematica, que será usado em modelagem, testes de

hipóteses e provas computacionais, e o Python, que será usado em manipulação de dados. A habilidade de traduzir problemas matemáticos abstratos em linguagem computacional fortalece a autonomia do pesquisador e sua capacidade de explorar grandes volumes de informação em busca de padrões relevantes que possam fundamentar avanços teóricos ou práticos.

Também é importante mencionar o desenvolvimento de habilidades de comunicação científica, tanto escrita quanto oral. O pesquisador será incentivado a registrar, apresentar e discutir suas descobertas, fortalecendo a clareza na exposição de argumentos matemáticos e na construção lógica de textos técnicos. Isso inclui o uso adequado de terminologias específicas, a redação de relatórios de progresso e a participação em seminários, encontros acadêmicos e discussões interdisciplinares enriquecedoras.

Por fim, será cultivada a capacidade de reflexão crítica sobre os limites e possibilidades da matemática aplicada, promovendo uma postura ética e responsável diante do uso de ferramentas matemáticas em contextos sensíveis, como a privacidade digital e a segurança cibernética. Assim, as habilidades desenvolvidas ao longo do plano não apenas fortalecem a formação acadêmica, mas também capacitam o pesquisador a atuar de forma inovadora, crítica e ética nos campos interligados da matemática, computação e sociedade.

REFERÊNCIAS BIBLIOGRÁFICAS

LUDWIG, Lara; REBELATTO, Miguel Grando; SILVA, Sandro José Ribeiro. **O estado da arte das criptografias modernas: uma revisão sistemática da literatura.** Revista Brasileira de Computação Aplicada (Canoas), v. 12, n. 2, p. 46-53, jun. 2020.
Disponível em: https://seer.upf.br/index.php/rbca/article/view/10455
Data de acesso: 2025-06-12

PAIVA, Carlos Daniel Chaves et al. **A busca pela prova da conjectura de Goldbach: explorando suas conquistas.** Revista Caderno Pedagógico – Studies Publicações e Editora Ltda., Curitiba, v. 21, n. 7, p. 01-28, 2024. DOI: 10.54033/cadped 21 7-134. Disponível em: https://studiespublicacoes.com.br/index.php/cadernopedagogico.
Acesso em: 2025-07-06

MOLLIN, Richard A. ***Números inteiros e criptografia.*** Tradução de Maria José Pacífico. 2. ed. São Paulo: Editora Ciência Moderna, 2005.

CRONOGRAMA DE EXECUÇÃO DO PROJETO

Mês 1

Definição final do escopo da pesquisa e delimitação precisa do problema.

Elaboração do projeto detalhado.

Levantamento preliminar de fontes bibliográficas iniciais.

Mês 2

Início da revisão bibliográfica sistemática sobre:

Criptografia, Teoria dos Números, Conjectura de Goldbach e Números primos.

Organização dos materiais por temas e autores.

Mês 3

Continuação da revisão bibliográfica.

Identificação e estudo dos principais algoritmos criptográficos baseados em números primos, com foco no RSA.

Mês 4

Estudo aprofundado da Conjectura Forte de Goldbach e dos resultados intermediários, como o método de Hardy-Littlewood, método de Vinogradov e teorema de Chen Jingrun.

Relacionamento desses resultados com a distribuição de primos.

Mês 5

Sistematização da bibliografia coletada.

Análise das possíveis relações entre a Teoria dos Números e algoritmos de criptografia.

Início da redação do capítulo teórico da pesquisa.

Mês 6

Estudo técnico e matemático da cifra RSA.

Análise da estrutura da chave pública e da dificuldade de fatoração.

Levantamento de vulnerabilidades teóricas baseadas em primos.

Mês 7

Formulação de hipóteses sobre possíveis vulnerabilidades futuras em algoritmos como o RSA, considerando avanços na matemática dos primos.

Redação parcial do capítulo analítico.

Mês 8

Estudo de algoritmos alternativos e considerados mais seguros, como os baseados em:

Problema do logaritmo discreto em grupos não convencionais, problemas de Lattice, isogenias de curvas elípticas e problemas combinatórios não estruturados.

Mês 9

Análise das consequências da descoberta de vulnerabilidades.

Impactos na segurança da informação, consequências sociais e políticas, e relevância na proteção de dados pessoais e institucionais.

Mês 10

Redação da seção de discussão.

Proposição de soluções e direções alternativas para algoritmos criptográficos.

Revisão parcial do texto produzido até aqui.

Mês 11

Conclusão da redação do trabalho completo.

Normalização das referências conforme ABNT.

Revisão técnica e textual da pesquisa.

Mês 12

Revisão final do projeto de pesquisa.

Preparação da apresentação (se aplicável).

Entrega oficial do trabalho.