Research, Society and Development, v. 14, n. 10, e63141049705, 2025
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v14i10.49705

Teoria dos números e aplicações criptográficas: A fatoração de primos na segurança digital

Number theory and cryptographic applications: Prime factorization in digital security

Teoría de números y aplicaciones criptográficas: La factorización de primos en la seguridad digital

Recebido: 02/10/2025 | Revisado: 08/10/2025 | Aceitado: 08/10/2025 | Publicado: 11/10/2025

Elijakson Rafael Lima de Souza
ORCID: https://orcid.org/0009-0007-5881-0101
Instituto Federal de Pernambuco, Brasil
E-mail: elijakson.rafael@gmail.com
Márcia Maria da Silva
ORCID: https://orcid.org/0000-0001-8839-8735
Instituto Federal de Pernambuco, Brasil
E-mail: marcia.msilva05@hotmail.com
Noberto Ferreira Xavier
ORCID: https://orcid.org/0009-0003-4701-6616
Instituto Federal de Pernambuco, Brasil
E-mail: nobertonx@gmail.com
Ozilan Viana Brandão
ORCID: https://orcid.org/0009-0003-3571-4038
Instituto Federal de Pernambuco, Brasil
E-mail: ozilanviana@gmail.com

Resumo
Dada a nossa forte dependência de computadores e recursos online, a proteção de dados tornou-se crucial. A Teoria dos Números, em especial a fatoração em primos, desempenha um papel fundamental nos sistemas de criptografia atuais, como o RSA, garantindo que as informações sejam mantidas confidenciais e autênticas. Este estudo objetiva examinar como a fatoração em primos é empregada na criptografia, abordando métodos para fatorar, o funcionamento do RSA, suas limitações e o impacto de computadores quânticos. Foi abordada também a necessidade de criptografia resistente a ataques quânticos e como integrar diferentes áreas como matemática, tecnologia e regulamentação. Os resultados indicam que a matemática não só suporta a segurança digital, mas também precisa se adaptar continuamente devido às novas tecnologias e aos perigos que surgem. Por isso, a pesquisa e o desenvolvimento de novas estratégias de segurança são indispensáveis.
Palavras-chave: Teoria dos Números; Fatoração de primos; Criptografia; RSA; Criptografia pós-quântica.

Abstract
Given our strong dependence on computers and online resources, data protection has become crucial. Number Theory, especially prime factorization, plays a fundamental role in current cryptographic systems such as RSA, ensuring that information remains confidential and authentic. This study aims to examine how prime factorization is employed in cryptography, addressing factoring methods, the functioning of RSA, its limitations, and the impact of quantum computers. It also addressed the need for encryption resistant to quantum attacks and the integration of different fields such as mathematics, technology, and regulation. The results indicate that mathematics not only supports digital security but also needs to continuously adapt to new technologies and emerging threats. Therefore, research and the development of new security strategies are indispensable.
Keywords: Number Theory; Prime factorization; Cryptography; RSA; Post-Quantum cryptography.

Resumen
Dada nuestra fuerte dependencia de los ordenadores y los recursos en línea, la protección de los datos se ha vuelto crucial. La Teoría de Números, especialmente la factorización en primos, desempeña un papel fundamental en los sistemas criptográficos actuales, como el RSA, garantizando que la información se mantenga confidencial y auténtica. Este estudio tiene como objetivo examinar cómo se emplea la factorización en primos en la criptografía, abordando métodos de factorización, el funcionamiento del RSA, sus limitaciones y el impacto de los ordenadores cuánticos. También se abordó la necesidad de una criptografía resistente a los ataques cuánticos y la integración de diferentes áreas como la matemática, la tecnología y la regulación. Los resultados indican que la matemática no solo sustenta la

seguridad digital, sino que también necesita adaptarse continuamente a las nuevas tecnologías y a los peligros emergentes. Por ello, la investigación y el desarrollo de nuevas estrategias de seguridad son indispensables.
Palabras clave: Teoría de Números; Factorización de primos; Criptografía; RSA; Criptografía post-cuántica.

1. Introdução

Na era digital, a proteção de dados é uma preocupação central. Transações bancárias e comunicações governamentais dependem da segurança da informação confidencial. A criptografia desempenha um papel importante, protegendo a confidencialidade, autenticidade e integridade das mensagens.

Vários sistemas de criptografia modernos, como os de chave pública, baseiam-se em conceitos da Teoria dos Números. O Teorema Fundamental da Aritmética, que estabelece que cada número inteiro pode ser fatorado de uma maneira única em primos, é um conceito central. A dificuldade de fatorar grandes números inteiros é um problema matemático importante.

A dificuldade de efetuar a fatoração na prática para números grandes é um ponto explorado por algoritmos como o RSA. A segurança do RSA reside na dificuldade de fatorar números grandes em seus primos. Este artigo examina a relação entre a Teoria dos Números e a criptografia moderna, com foco no uso da fatoração em primos. Os fundamentos matemáticos da criptografia assimétrica serão apresentados, algoritmos de fatoração serão abordados e os problemas que surgem com tecnologias como a computação quântica serão mencionados.

Esta análise procura explicitar o uso de conceitos da Matemática Pura em tecnologias que impactam a sociedade. Ao unir Teoria dos Números e criptografia, este estudo busca explicitar a relevância da matemática teórica para a segurança digital global.

Este estudo examina detalhadamente como a fatoração em primos é empregada na criptografia, abordando métodos para fatorar, o funcionamento do RSA, suas limitações e o impacto de computadores quânticos.

2. Metodologia

Realizou-se uma pesquisa mista envolvendo investigação de natureza qualitativa e quantitativa, incluindo simulações, investigação documental de fonte direta em documentos sobre matemática e indireta (Pereira et al., 2018), em pesquisa bibliográfica e não sistemática narrativa (Rother, 2007).

Neste estudo, foi realizada uma pesquisa em livros, artigos e documentos sobre matemática, criptografia e agências reguladoras.

A abordagem metodológica envolveu:

1. Pesquisa: Coletamos dados de livros de Teoria dos Números (Burton, 2011; Hardy & Wright, 2008), textos sobre criptografia atual (Stallings, 2017; Rivest, Shamir & Adleman, 1978) e estudos de criptografia pós-quântica (NIST, 2022; Shor, 1997).

2. Análise: Examinamos conceitos matemáticos importantes, como números primos e métodos de fatoração, para entender como eles contribuem para a proteção da criptografia.

3. Exemplos: Analisamos como o algoritmo RSA funciona, mostrando como a fatoração de primos cria chaves e protege mensagens.

4. Discussão: Avaliamos os problemas, as dificuldades de uso, o potencial da computação quântica e o futuro da criptografia pós-quântica.

5. Conclusão: Integramos o conhecimento obtido na teoria e na prática para fornecer uma visão abrangente de como a Teoria dos Números contribui para a segurança da informação, oferecendo sugestões e indicando direções para pesquisas

futuras.

Por meio dessa abordagem metodológica, conectamos a matemática teórica com a prática na segurança digital, realçando a importância dessa área para a ciência e para a tecnologia.

3. Resultados e Discussão

Esta análise explora a decomposição de números inteiros em primos, essencial na matemática e base da criptografia moderna. Para clareza e para apresentar as complexidades do tópico, as principais conclusões e discussões estão organizadas por seções temáticas.

3.1 Fundamentos Matemáticos da Fatoração

O Teorema Fundamental da Aritmética afirma que todo número inteiro maior que um pode ser escrito de um jeito único como um produto de números primos. Talvez pareça simples, mas essa ideia tem usos importantes, porque a dificuldade de fatorar números grandes é a base de muitos sistemas de segurança de dados atuais. Fatorar números pequenos não é muito complicado, mas a dificuldade aumenta rápido conforme o número cresce, tornando impossível para computadores normais.

Essa dificuldade não é só um problema matemático. Ela é usada, por exemplo, no método RSA, onde dois primos são multiplicados para criar um número que é quase impossível de fatorar. Isso mantém a chave secreta e informações importantes protegidas, mostrando como ideias matemáticas podem ser usadas para proteger dados na prática.

Um ponto interessante sobre os números primos é que eles aparecem de forma irregular. Essa falta de um padrão que se possa prever aumenta a dificuldade dos métodos de fatoração e, consequentemente, a segurança dos sistemas de proteção de dados. Assim, a teoria dos números, além de ser importante por si só, apoia soluções essenciais para a segurança digital.

3.2 Algoritmos de Fatoração e Desempenho Computacional

O estudo analisou métodos de fatoração numérica, observando seus pontos fortes e fracos e seu impacto na segurança dos sistemas criptográficos. A fatoração por tentativa, um método introdutório, só funciona bem com números pequenos, tornando-se ineficaz à medida que o tamanho aumenta. O método de Fermat é útil quando os fatores estão próximos, mas não é adequado para números grandes escolhidos aleatoriamente, sendo necessário recorrer a métodos mais avançados.

O método da peneira quadrática é útil para números de até 100 dígitos e bastante comum no ensino superior para testar a fatoração. Para números bem maiores, o método GNFS (General Number Field Sieve) é mais apropriado, embora possua limitações, não permitindo a fatoração de números excessivamente grandes. Esta análise indica que sistemas como o RSA permanecem seguros para chaves de tamanho adequado.

A pesquisa avaliou a abordagem mais adequada e os recursos computacionais exigidos para os algoritmos. Os sistemas de criptografia atuais precisam considerar a teoria da fatoração e as capacidades computacionais, garantindo que as chaves selecionadas resistam a ataques sofisticados. A relação entre matemática e tecnologia explicita a importância do planejamento e de boas práticas em sistemas de criptografia.

3.3 Aplicações Práticas do RSA

O RSA explicita como a fatoração de números primos auxilia na criptografia cotidiana. Observamos como as chaves são geradas, como as mensagens são codificadas e decodificadas, e como é imprescindível selecionar números primos grandes e aleatórios. Gerar essas chaves exige cálculos complexos, fazendo com que a obtenção da chave privada seja muito difícil se o agente não possuir os primos originais.

Utilizamos exemplos simplificados com números pequenos para exemplificar o funcionamento do sistema, esclarecendo que a segurança real demanda primos realmente extensos. Observamos como o RSA protege as informações, possibilita confirmar o remetente da mensagem e assinar as mensagens, ampliando o emprego da Teoria dos Números em diversas situações.

Ressaltamos que é necessário cautela ao empregar o algoritmo. Se ocorrer alguma falha, como na geração dos primos ou na gestão das chaves, a segurança do sistema pode ser comprometida. Por isso, mesmo com uma teoria robusta, a cautela e a verificação constante são elementos importantes para manter a informação segura.

3.4 Limitações e Vulnerabilidades

Embora o RSA e outros sistemas baseados na fatoração de números primos possuam uma base teórica consistente, eles apresentam vulnerabilidades na prática. Chaves pequenas podem ser quebradas por ataques de força bruta, e a seleção previsível de primos aumenta o risco de falhas de segurança. Ataques que exploram características físicas de dispositivos explicitam que a matemática por si só não assegura proteção total.

A dificuldade de fatoração é um ponto fundamental. Com o avanço da tecnologia, principalmente na computação quântica, algoritmos como o RSA podem se tornar vulneráveis. Isso requer a adoção de métodos combinados ou a transição para a criptografia pós-quântica. A análise também apontou que a atualização contínua de sistemas legados é crucial para evitar falhas de segurança.

A capacitação de profissionais, auditorias frequentes e políticas internas são relevantes para atenuar a probabilidade de problemas. Não é suficiente confiar na teoria; é importante aliar tecnologia, treinamento e políticas para garantir a segurança em larga escala.

3.5 Ameaças da Computação Quântica

A computação quântica representa uma transformação expressiva na segurança digital. O algoritmo de Shor revela que computadores quânticos conseguem fatorar números inteiros extensos com agilidade, comprometendo a segurança de sistemas como o RSA e invalidando diversas práticas de criptografia atuais. A pesquisa indicou que, embora ainda em fase experimental, a computação quântica demanda um planejamento estratégico e estudo em criptografia resistente.

Além da ameaça direta à fatoração, a computação quântica causa impacto na integridade dos sistemas de assinatura digital e autenticação. A análise mencionou que organizações e governos devem se preparar para adotar criptografia pós-quântica e abordagens híbridas com o objetivo de mitigar riscos futuros. Essa preparação engloba padronização, adaptação de protocolos e investimento em pesquisa aplicada.

Em síntese, a pesquisa constatou que a convergência de matemáticos, cientistas da computação e profissionais de segurança é crucial para assegurar uma mudança segura para a era quântica. A cooperação multidisciplinar se mostra fundamental para criar algoritmos seguros, compatíveis com os sistemas existentes e resistentes a ataques cibernéticos emergentes.

3.6 Criptografia Pós-Quântica e Tendências Futuras

O estudo especificou que a criptografia pós-quântica (PQC) apresenta opções viáveis, como algoritmos que empregam reticulados, códigos que corrigem erros, funções hash e sistemas multivariáveis. O objetivo desses métodos é assegurar a segurança mesmo quando computadores quânticos conseguirem efetuar a fatoração de números primos.

A pesquisa também indicou que implementar a PQC requer planejamento das instituições, padronização dos

protocolos e preparo dos profissionais de TI. Mudar os sistemas antigos de forma gradual é substancial para não criar brechas durante a mudança. Empregar soluções mistas, que combinam algoritmos atuais e pós-quânticos, é uma forma de ter segurança enquanto a tecnologia quântica ainda está em desenvolvimento.

Por fim, a pesquisa lembrou que é necessário continuar buscando inovação continuamente. Criar algoritmos novos, ter estratégias de cripto-agilidade e fazer auditorias recorrentes serão ações importantes para garantir que os sistemas de informação continuem seguros em um mundo tecnológico em constante transformação.

3.7 Integração entre Teoria, Prática e Instituições

A análise revelou que a segurança digital depende da união de três elementos fundamentais: teoria matemática, tecnologia aplicada e regulamentações institucionais. A Teoria dos Números fornece o alicerce teórico; a aplicação correta garante que tudo funcione adequadamente; e regras e padrões internacionais promovem uniformidade, compatibilidade e segurança em escala global.

O estudo apresentou exemplos de como normas, como as do NIST, auxiliam na seleção de algoritmos seguros, estimulam a mudança para soluções pós-quânticas e incentivam auditorias recorrentes. Essa união é fundamental para atenuar riscos que emergem, como falhas na aplicação e novas ameaças tecnológicas.

Por fim, a pesquisa apontou que unir teoria, prática e instituições é um ponto forte para empresas, governos e organizações, garantindo que os sistemas de criptografia permaneçam firmes, confiáveis e aptos a se adaptar a novas necessidades tecnológicas e ameaças que possam surgir.

3.8 Cálculos e Demonstrações (Apêndice Numérico)

3.8.1 Objetivo desta seção

Esta subseção traz cálculos completos e demonstrativos que conectam diretamente a Teoria dos Números à aplicação criptográfica — especialmente ao RSA — e apresenta exemplos de métodos de fatoração e testes de primalidade. O objetivo é fornecer material numérico rigoroso para inclusão no corpo do artigo ou no apêndice técnico, permitindo avaliação matemática e reprodutibilidade por banca examinadora.

3.8.2 Propriedades básicas (lemmas usados)

- **Teorema Fundamental da Aritmética:** todo inteiro $n > 1$ admite decomposição única em primos (até ordem).
- **Lema de Euler / Teorema de Eulerx:** se gcd $(a,n) = 1$, então $a^{\varphi(n)} \equiv 1 \pmod{n}$, onde φ é a função totiente de Euler.
- **Lema (uso no RSA):** se $n = pq$ com p, q primos e $ed \equiv 1 \pmod{\varphi(n)}$, então $M^{ed} \equiv M \pmod{n}$ para todo M com gcd $(M,n) = 1$.

Esses resultados justificam a correção teórica do RSA e são usados nas demonstrações numéricas abaixo.

3.8.3 Exemplo completo do RSA (cálculo passo-a-passo e otimização por CRT)

Escolha de primos (didática): Escolhemos primos razoavelmente pequenos para viabilizar todos os passos manualmente, mantendo a didática sem perder rigor:

$$p = 61;\ q = 53$$

Cálculo de n e φ (n):

$$n = p \cdot q = 61 \times 53 = 3.233.$$

$$\varphi(n) = (p - 1)\,(q\text{-}1) = 60 \times 52 = 3.120$$

Escolha de e: tomamos e = 17 (verifica-se gcd (17, 3120) =1).

Cálculo de d (inverso modular de e módulo φ(n)) — Algoritmo de Euclides Estendido (passos):

Realizamos a divisão sucessiva para obter o gcd e, em seguida, voltamos substituindo para achar a combinação linear:

$$3.120 = 17 \text{ x } 183 + 9,$$

$$17 = 9 \text{ x } 1 + 8,$$

$$9 = 8 \text{ x } 1 + 1,$$

$$8 = 1 \text{ x } 8 + 0.$$

Voltando (substituições para o Bézout), obtém-se:

$$1 = 2 \text{ x } 9 - 17 = 2\,(3.120 - 17 \text{ x } 183) - 17 = 2 \text{ x } 3.120 - 367 \text{ x } 17$$

Portanto – 367 x 17 + 2 x 3.120 = 1 e o inverso de 17 módulo 3.120 é -367 ≡ 2.753 (mod 3.120)

Logo:

$$d = 2.753$$

Par de chaves:

Chave pública: $(n,e) = (3.233, 17)$

Chave privada: $(n,d) = (3.233, 2.753)$

Exemplo de encriptação (exponenciação modular com square-and-multiply):

Escolha da mensagem $M = 65$ (representação numérica). Queremos $C \equiv M^{\wedge}e \pmod{n}$.

Para reduzir cálculos, usamos potências de 2:

$$65^1 \equiv 65 \pmod{3.233},$$

$$65^2 \equiv 65^2 = 4.225 \equiv 992 \pmod{3.233},$$

$$65^{\wedge}4 \equiv 992^2 = 984.064 \equiv 1.233 \pmod{3.233}$$

$$65^{\wedge}8 \equiv 1.232^2 \equiv 1.547 \pmod{3.233}$$

$$65^{\wedge}16 \equiv 1.547^2 \equiv 789 \pmod{3.233}$$

Como $e = 17 = 16 + 1$

$$65^{\wedge}17 \equiv 65^{\wedge}16 \text{ x } 65 \equiv 789 \text{ x } 65 \equiv 2.790 \pmod{3.233}$$

Logo o cifrado é:

$$C = 2.790$$

Decriptação: $M \equiv C^{\wedge}d \pmod{n}$ (verificação):

Na prática, calcular $C^{\wedge}2753$ diretamente é custoso; usa-se novamente exponenciação modular por quadrados (ou CRT – abaixo). A propriedade $M^{\wedge}ed \equiv M \pmod{n}$ garante que a decriptação devolve 65. Computacionalmente confirma-se $C^{\wedge}2753 \bmod 3.233 = 65$.

Aceleração via CRT (Chinese Remainder Theorem):

Para eficiência, calcula-se decriptação módulo p e q e reconstrói-se o resultado:

$$d_p = d \bmod (p - 1) = 2.753 \bmod 60 = 53,$$

$$dq = d \bmod (q - 1) = 2.753 \bmod 52 = 49.$$

Calcule:

$$m1 \equiv C^{dp} \bmod p = 2790^{53} \bmod 61 = 4;$$
$$m2 \equiv C^{dq} \bmod q = 2790^{49} \bmod 53 = 12;$$

Encontre $q^{-1} \bmod p$. Aqui $q = 53$, $p = 61$. Verifica-se $53 \times 38 \equiv 2.014 \equiv 1 \pmod{61}$, então $q^{-1} = 38$.

Calcule:

$h \equiv q^{-1} \times (m1 - m2) \bmod p = 38 \times (4 - 12) \bmod 61 = 38 \times (-8) \bmod 61 \equiv 1$.

Finalmente:

$$m \equiv m2 + h \times q = 12 + 1 \times 53 = 65,$$

recuperando a mensagem original. A aplicação do CRT reduz substancialmente o custo de cálculo, pois as exponenciações são feitas em módulos menores (p e q).

3.8.4 Método de Fermat — exemplo prático

O método de Fermat é eficiente quando os fatores são próximos. Dado N, procuramos $a = \lceil \sqrt{N} \rceil$ tal que $a^2 - N$ seja quadrado perfeito.

Exemplo: $N = 8.051$.

$$\sqrt{8051} \approx 89,78 \Rightarrow a = 90$$
$$a^2 - N = 90^2 - 8.051 = 8.100 - 8.051 = 49 = 7^2$$

Portanto:

$$8.051 = a^2 - b^2 = (a - b)(a + b) = (90 - 7)(90 + 7) = 83 \times 97.$$

Fermat fatorou 8.051 em apenas uma iteração neste caso, ilustrando a eficiência do método quando fatores são moderadamente próximos.

3.8.5 Pollard–Rho — demonstração curta (iteração)

Pollard–Rho é um método probabilístico eficiente em muitos casos para encontrar um divisor não-trivial.

Usando $N = 8.051$, função $f(x) = x^2 + 1 \pmod N$, início x0 = y0 = 2:

Iterações iniciais (tortoise & hare):

$x1 = f(2) = 5$; $y1 = f(f(2)) = f(5) = 26$ x $gcd(|5-26|; 8.051) = gcd(21, 8.051) = 1$.

$x2 = f(5) = 26$; $y2 = f(f(26)) = f(677) = 7.474$ x $gcd(|26-7.474|, 8.051) = 1$.

$x3 = f(26) = 677$; $y3 = f(f(7.474)) = f(871) = 871$. Agora $gcd(|677 - 871|, 8.051) = gcd(194; 8.051) = 97$.

Encontrou-se o fator 97 na terceira iteração. Assim, Pollard–Rho demonstrou rapidez prática nesse caso. (Observação: o método é probabilístico e pode necessitar reinício com outro parâmetro c se $gcd = N$.)

3.8.6 Teste de primalidade (Miller–Rabin) — exemplo

Miller–Rabin é um teste probabilístico usado para gerar e verificar primos na geração de chaves.

Exemplo: testar $n = 101$ com base $a = 2$.

Decomponha $n - 1 = 100 = 2^8 \times d$ com d ímpar:

$100 = 2^2 \times 25 \Rightarrow s = 2, d = 25$.

Calcule $x = 1$ *ou* $x = n - 1$ então provavelmente primo; aqui $x = 10$. Faça as iterações de quadrado:

$x1 = x^2 \bmod n = 10^2 \bmod 101 = 100 \equiv -1 \pmod{101}$

Como alcançamos $n - 1$ em uma das iterações, o teste declara **provavelmente primo** para a base 2. Repetir com outras bases reduz a probabilidade de falso positivo (para utilização prática, faz-se várias iterações de Miller–Rabin).

3.8.7 Complexidade prática e recomendações de tamanho de chave

Tentativa direta (força bruta): custo $O(\sqrt{N})$.

Fermat / Pollard–Rho: bom para certos casos ou números com fatores específicos; Pollard–Rho tem custo esperado aproximadamente $O(N^{1/4})$ em muitos casos práticos.

Crivagem Quadrática: eficaz até ~100 dígitos.

GNFS (General Number Field Sieve): melhor algoritmo clássico conhecido para grandes inteiros; complexidade heurística subexponencial $Ln[1/3, c]$.

Shor (quântico): tempo polinomial; se computadores quânticos escaláveis existirem, quebra as bases fatoração/elog discreto.

Recomendações práticas (orientativas):

- Não usar RSA < 1024 bits (inseguro hoje).
- 2048 bits é atualmente o mínimo recomendado para segurança razoável.
- Para proteção de longo prazo (dados sensíveis por décadas), considerar 3072–4096 bits ou migração para primitives pós-quânticas.
- Implementar geração de primos por teste probabilístico (Miller–Rabin com repetições suficientes) e garantir entropia no RNG.

4. Conclusão

A análise deste estudo explicita que a Teoria dos Números, em especial a fatoração de inteiros em primos, possui um papel crítico na segurança digital contemporânea. Ao examinar o algoritmo RSA e as aplicações da fatoração, constatamos que conceitos matemáticos abstratos afetam diretamente tecnologias cruciais, garantindo a confidencialidade, integridade e autenticidade de informações em escala global.

Os resultados indicam que a segurança dos sistemas criptográficos de chave pública depende da consistência teórica do algoritmo e de fatores práticos, como o tamanho apropriado das chaves, a seleção criteriosa dos números primos e a execução adequada do sistema. Se algum desses aspectos apresentar falhas, toda a segurança pode ser comprometida, evidenciando a necessidade de práticas rigorosas de desenvolvimento e monitoramento.

Este estudo ressalta que a computação quântica representa uma ameaça à criptografia tradicional baseada na fatoração de primos. O Algoritmo de Shor sugere que computadores quânticos poderosos conseguem quebrar a segurança de sistemas como o RSA rapidamente, tornando urgente a pesquisa e o emprego de algoritmos pós-quânticos. Estratégias de mudança, cripto-agilidade e soluções mistas são importantes para manter a segurança das informações em um cenário tecnológico em rápida evolução.

Outro ponto importante é a conexão da matemática pura com a tecnologia prática. A pesquisa reforça que áreas abstratas, como a Teoria dos Números, possuem aplicações reais e relevantes na sociedade digital, impactando finanças, comunicação, governo e privacidade. Essa junção de teoria e prática demonstra que é necessário investir em programas acadêmicos e pesquisas científicas que integrem conhecimento matemático com aplicações tecnológicas.

Além do âmbito técnico, é crucial considerar políticas e regulamentações, como as estabelecidas pelo NIST, para orientar a adoção segura de algoritmos e a mudança para criptografia resistente a ataques quânticos. Instruir profissionais continuamente, criar padrões de processos e atentar para pontos fracos na execução são aspectos relevantes para garantir a confiança em sistemas criptográficos.

Em resumo, as conclusões deste estudo são:

1. A fatoração de números primos é a base matemática da criptografia de chave pública e garante segurança se for feita corretamente.
2. A segurança do RSA e de sistemas parecidos depende da teoria e de boas práticas de execução e manutenção.
3. A tecnologia, como a computação quântica, traz desafios que pedem soluções novas e planejamento.
4. Integrar teoria matemática, tecnologia e regulamentação é imprescindível para manter a segurança da informação confiável.
5. Realizar pesquisas contínuas em criptografia e Teoria dos Números é importante para que a matemática pura continue a fornecer soluções para problemas do mundo real.

Este estudo confirma que a Teoria dos Números é uma ferramenta para a sociedade digital e que se preparar para ameaças é fundamental para proteger as informações no século XXI. O avanço do conhecimento matemático, aliado à aplicação tecnológica, alicerça a segurança e a inovação nos sistemas de informação.

Referências

Burton, D. M. (2011). *Elementary Number Theory*. (7.ed). New York: McGraw-Hill

Cox, D. A. (2013). *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. (2. ed.). Hoboken: Wiley, 2013.

Hardy, G. H. & Wright, E. M. (2008). *An Introduction to the Theory of Numbers*. (6.ed). Oxford: Oxford University Press.

Katz, J. & Lindell, Y. (2014). *Introduction to Modern Cryptography*. (2.ed). Chapman & Hall/CRC.

Lenstra, A. K. & Verheul, E. R. (2001). *Selecting Cryptographic Key Sizes*. Journal of Cryptology. 14(4), 255–93.

Miller, G. L. (1976). *Riemann's Hypothesis and Tests for Primality*. Journal of Computer and System Sciences. 13(Issue 3), 300-17.

NIST. (2022). *Post-Quantum Cryptography Standardization*. National Institute of Standards and Technology.

Pereira, A. S. et al. (2018). Metodologia da pesquisa científica. [free ebook]. Santa Maria. Editora da UFSM.

Pollard, J. M. (1975). *A Monte Carlo Method for Factorization of Integers*. Mathematics of Computation. Scientific Notes. 15, 331–4.

Rabin, M. O. (1980). *Probabilistic Algorithm for Testing Primality*. Journal/Conference (Miller–Rabin test variants).

Rivest, R., Shamir, A. & Adleman, L. (1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM. 21(2), 120-6.

Rosen, K. H. (2011). *Elementary Number Theory and Its Applications*. (6.ed). Pearson.

Rother, E. T. (2007). Revisão sistemática x revisão narrative. Acta Paulista de Enfermagem. 20(2), 5-6.

Shor, P. W. (1997). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing. 26(5), 1484–509.

Singh, S. (2000). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. (7.ed). Pearson.

Stewart, I. & Tall, D. (2015). *Algebraic Number Theory and Fermat's Last Theorem*. (4.ed). Boca Raton: CRC Press.

Stinson, D. R. & Paterson, M. B. (2018). *Cryptography: Theory and Practice*. (4.ed). Chapman & Hall/CRC.