FATORAÇÃO DE INTEIROS ASSISTIDA POR REDE NEURAL: APRIMORANDO A FATORAÇÃO EM ALGORITMO DE CRIPTOGRAFIA ASSIMÉTRICA POR MEIO DE METODOLOGIA HÍBRIDA

NEURAL NETWORK-ASSISTED INTEGER FACTORIZATION: IMPROVING FACTORIZATION IN ASYMMETRIC ENCRYPTION ALGORITHMS THROUGH HYBRID METHODOLOGIES

FACTORIZACIÓN DE ENTEROS ASISTIDA POR REDES NEURONALES: MEJORANDO LA FACTORIZACIÓN DE ALGORITMOS DE CIFRADO ASIMÉTRICO MEDIANTE METODOLOGÍA HÍBRIDA

Felipe Jordão Silva[1]

Resumo

A criptografia assimétrica, muito utilizada em diversos sistemas, trouxe mais segurança através de problemas matemáticos complexos, como o problema de fatoração de inteiros com objetivo de garantir a integridade e confidencialidade dos dados, entretanto, com a evolução rápida do poder computacional, cresce a preocupação em relação a essa robustez dos algoritmos tradicionais contra ameaças emergentes, particularmente aquelas representadas pela computação quântica. O presente artigo tem como objetivo apresentar uma abordagem alternativa para aperfeiçoar o processo de fatoração de chaves públicas que utilizam criptografia assimétrica, em específico a criptografia RSA, através de uma união de técnicas de aprendizado de máquina e métodos tradicionais de fatoração. Este estudo propõe uma metodologia híbrida por meio da aplicação de uma rede neural para prever fatores primos candidatos, complementada por um algoritmo de verificação de primalidade probabilístico. Uma comparação de desempenho entre métodos é realizada, avaliando eficácia e eficiência computacional, os resultados desta pesquisa contribuirão para os esforços contínuos para otimizar a fatoração em algoritmos RSA.

Palavras-Chave: criptografia assimétrica; redes neurais; fatoração de números; aprendizado de máquina.

Abstract

Asymmetric cryptography, widely used in various systems, has brought more security through complex mathematical problems, such as the integer factorization problem, with the aim of guaranteeing data integrity and confidentiality. However, with the rapid evolution of computing power, concerns are growing regarding the robustness of traditional algorithms against emerging threats, particularly those posed by quantum computing. This article aims to present an alternative approach to improve the public key factorization process that uses asymmetric cryptography, specifically RSA cryptography, through a combination of machine learning techniques and traditional factorization methods. This study proposes a hybrid methodology through the application of a neural network to predict candidate prime factors, complemented by a probabilistic primality verification algorithm. A performance comparison, between methods, is performed, evaluating computational effectiveness and efficiency. The results of this research will contribute to ongoing efforts to optimize factorization in RSA algorithms.

Keywords: asymmetric cryptography; neural networks; number factorization; machine learning.

[1] Aluno do curso dd bacharelado em Ciência da Computação do Centro Universitário Internacional. Formado em Gestão da Defesa e Segurança Cibernética pelo Centro Universitário Internacional. Pós-graduado em estudos matemáticos aplicados a tópicos da física pela Faculdade Focus. https://orcid.org/0009-0002-5683-1164. http://lattes.cnpq.br/7323494332905664.

DOI: https://doi.org/10.22169/cadprog.v5n9.3592

Resumen

La criptografía asimétrica, ampliamente utilizada en varios sistemas, ha aportado mayor seguridad a través de problemas matemáticos complejos, como el problema de factorizar enteros para garantizar la integridad y confidencialidad de los datos; sin embargo, con la rápida evolución de la potencia computacional, existe una creciente preocupación por la robustez de los algoritmos tradicionales frente a amenazas emergentes, especialmente aquellas representadas por la computación cuántica. Este artículo pretende presentar un enfoque alternativo para mejorar el proceso de factorización de claves públicas que utilizan criptografía asimétrica, específicamente criptografía RSA, mediante la unión de técnicas de aprendizaje automático y métodos tradicionales de factorización. Este estudio propone una metodología híbrida mediante la aplicación de una red neuronal para predecir factores primos candidatos, complementada por un algoritmo probabilístico de verificación de primalidad. Se realiza una comparación de rendimiento entre métodos, evaluando la efectividad y eficiencia computacional; los resultados de esta investigación contribuirán a los esfuerzos continuos para optimizar la factorización en los algoritmos RSA.

Palabras clave: criptografía asimétrica; redes neuronales; factorización numérica; aprendizaje automático.

1 Introdução

A fatoração de inteiros é o processo pela qual ocorre a decomposição de um número composto em um produto de inteiros menores e há anos tem um papel fundamental nas teorias dos números e da criptografia, possuindo uma maior importância no campo da criptografia assimétrica, a segurança dos sistemas criptográficos de chave pública modernos depende fundamentalmente da intratabilidade computacional de certos problemas matemáticos, sendo a fatoração de inteiros fator fundamental do protocolo RSA (Rivest; Shamir; Adleman, 1978) e de esquemas de criptografia relacionados.

As abordagens tradicionais de fatoração de inteiros evoluíram da divisão por tentativas e do método Rho de Pollard para algoritmos sofisticados como Quadratic Sieve e o General Number Field Sieve (GNFS), atualmente o algoritmo de fatoração clássico mais eficiente conhecido para inteiros grandes (Pomerance, 1996). Embora esses métodos tenham alcançado notável sucesso teórico e prático, com o avanço da computação quântica, essa dificuldade apresenta um desafio para avanços na eficiência computacional e inovação.

A segurança de muitos algoritmos de criptografia assimétrica, incluindo RSA, depende fundamentalmente da dureza computacional da fatoração de números inteiros. À medida que a escala e a complexidade dos sistemas criptográficos continuam a se expandir, a necessidade de técnicas de fatoração aprimoradas torna-se cada vez mais crítica (Abudqa *et al.*,2020).

Nos últimos anos, tem aumentado o interesse na utilização de técnicas de aprendizado de máquina para repensar abordagens clássicas de fatoração, as redes neurais em particular, demonstram uma vantagem em reconhecimento de padrões, otimização e resolução de problemas complexos. Essas capacidades sugerem a possibilidade de utilização das redes neurais no auxílio da fatoração de inteiros. Estudos preliminares tem demonstrado que redes

neurais podem ser aplicadas para identificar padrões na estrutura dos números compostos e aproximar soluções para problemas de fatoração com maior eficiência do que métodos puramente algorítmicos (Murat; Kadyrov, 2021).

Este artigo faz uma exploração do potencial da fatoração de inteiros auxiliada por rede neural, propondo uma metodologia híbrida que faz uma combinação entre os pontos fortes dos algoritmos de fatoração clássicos, com as capacidades de aprendizagem adaptativa das redes neurais.

2 Fundamentação teórica

A criptografia assimétrica, também conhecida como criptografia de chave pública, é um pilar fundamental da segurança cibernética moderna, permitindo a comunicação segura e a proteção de dados em uma ampla gama de aplicações, do comércio eletrônico à defesa nacional (Grigoriev *et al.*,2009).

A característica principal do algoritmo é a geração de um par de chaves, isto é, uma chave pública para criptografar as mensagens e uma chave privada correspondente para decifrá-las. A chave pública é expressa em dois componentes, um módulo N, a qual é o produto de dois números primos grandes $P\ e\ Q$, e um expoente de criptografia.

A segurança do sistema resulta da dificuldade de fatorar N em seus componentes primos, $P\ e\ Q$, conhecendo apenas $N\ e\ E$. A criptografia RSA é realizada utilizando a chave pública, em que uma mensagem de texto simples P é transformada em texto cifrado C pela operação:

$$\mathrm{C} \equiv p^{E} \bmod N$$

A descriptografia, por outro lado, usa a chave privada, recuperando o texto simples por meio da operação:

$$p \equiv c^{D}\ mod\ N$$

Em que D é o inverso multiplicativo de E módulo de $\phi(N)(Almobin,2024)$.

No decorrer dos anos, vários métodos de fatoração foram propostos e adequados, desde o crivo quadrático até abordagens mais recentes baseadas em computação quântica,

entretanto para chaves criptográficas maiores como a de 2048 bits, a fatoração permanece computacionalmente inacessível pelos métodos tradicionais, mantendo sua resiliência.

Com o advento do aprendizado de máquina e, em particular, das redes neurais, houve uma expansão em diversas áreas de possibilidades para abordar problemas complexos, incluindo a área da criptografia, diversas pesquisas têm explorado a aplicação das técnicas de aprendizado de máquina na otimização de algoritmos criptográficos, demonstrando o potencial das abordagens na melhoria ou comprometimento da segurança dos algoritmos atuais.

As redes neurais, inspiradas no funcionamento do cérebro humano, tem demonstrado notável capacidade em resolver problemas complexos em diversos domínios, desde reconhecimento de padrões até otimização combinatória (Lecun *et al,* 2015).

A criptografia assimétrica, introduzida por Diffie e Hellman (1976), trouxe um grande avanço para o campo da criptografia ao propor um sistema onde as chaves de criptografia e descriptografia são distintas, mas matematicamente relacionadas. Este paradigma resolve o problema da distribuição segura de chaves, um dos principais desafios da criptografia simétrica tradicional. Ao contrário dos sistemas simétricos, onde a chave secreta compartilhada deve ser transmitida com segurança entre as partes, a criptografia assimétrica permite que uma chave pública seja distribuída livremente, enquanto a chave privada correspondente permanece segura por seu proprietário.

O algoritmo RSA é um dos exemplos mais proeminentes de criptografia assimétrica, sua segurança tem como base a dificuldade computacional de fatorar o produto de dois números primos grandes. Dado um número $N = P * Q$ onde P e Q são grandes primos, o desafio reside em encontrar $P\ e\ Q$ de forma eficiente conhecendo apenas N. A natureza assimétrica desse problema decorre do fato de que, embora a multiplicação de dois grandes primos seja computacionalmente trivial, acredita-se que a operação inversa de fatorar seu produto seja computacionalmente intratável para números suficientemente grandes usando algoritmos atualmente conhecidos (Rivest; Shamir; Adleman, 1978).

A complexidade computacional da fatoração de inteiros é classificada como NP (não-determinístico polinomial) (Garey e Johnson,1979). Essa classificação implica que, embora uma solução para o problema de fatoração possa ser verificada em tempo polinomial, nenhum algoritmo conhecido pode encontrar uma solução em tempo polinomial com relação ao tamanho da entrada em um computador clássico.

A busca por fatorar números inteiros de forma eficiente se estendeu por séculos, produzindo uma gama diversificada de algoritmos, cada um com seus pontos fortes e fracos.

O método mais simples, conhecido como divisão por teste, envolve testar sistematicamente divisores potenciais até a raiz quadrada do número a ser fatorado, embora seu conceito simples e facilmente replicável, a divisão por teste sofre de complexidade de tempo exponencial, tornando-se impraticável para fatorar números grandes, em particular aqueles empregados na criptografia RSA.

Por outro lado, o método de fatoração de Fermat, representa uma pequena melhoria em relação à divisão por tentativa, explorando a representação de um número ímpar como a diferença de dois quadrados, especificamente a identidade algébrica:

$$N = a^2 - b^2 = (a + b) \cdot (a - b)$$

Ao procurar interativamente por valores de tais que a^2 seja um quadrado perfeito, o algoritmo busca expressar N como o produto de dois fatores. Entretanto, ainda que o método de Fermat possa ser eficaz quando os fatores estão próximos um do outro, seu desempenho degrada significativamente quando os fatores estão distantes, tornando-o inadequado para fatoração de propósito geral.

Com os avanços na teoria dos números, algoritmos de fatoração mais sofisticados foram desenvolvidos. O crivo quadrático, desenvolvido por Carl Pomerance[2] em 1981 foi um dos primeiros algoritmos propostos para fatoração de números inteiros. O método proposto por Pomerance utiliza relações entre quadrados modulares para encontrar fatores, oferecendo um melhor desempenho em relação a divisão por tentativa para números grandes.

O crivo de corpo numérico (NFS) por outro lado, desenvolvido por Jhon Pollard em 1988 e posteriormente melhorado por outros pesquisadores, atualmente é o algoritmo mais eficiente que se tem conhecimento para fatoração de números inteiros grandes. Esse método utiliza técnicas avançadas da teoria algébrica dos números e tem sido utilizado com frequência para fatoração de números maiores em criptografia RSA.

Em paralelo aos avanços de algoritmos de fatoração, testes de primalidade probabilísticos vêm ganhando relevância devido à sua eficiência e confiabilidade. O teste de Miller-Rabin, tornou-se amplamente utilizado na prática criptográfica. Esse teste pode determinar se um número é composto de fato ou se é provavelmente primo com alta probabilidade, repetido por diversas vezes para aumentar a confiança no resultado.

Com o surgimento de técnicas de aprendizado de máquina, mais especificamente as redes neurais, se introduziu novas abordagens para problemas de reconhecimento de padrões

[2] Professor emérito do departamento de matemática da universidade de Darmouth, possui contribuições fundamentais no campo da teoria dos números. Disponível em: https://math.dartmouth.edu/~carlp/ Acesso em: 13 mar. 2025.

anteriormente considerados inacessíveis por meios algorítmicos convencionais. Pesquisas tem demonstrado que redes neurais podem reconhecer certos padrões estruturais no processo de fatoração, trazendo uma potencial aceleração em fases específicas de algoritmos.

As redes neurais vêm se destacando como ferramentas promissoras devido à sua capacidade de modelar funções altamente não lineares e explorar eficientemente espaços de solução complexos (Jansen; Nakayama, 2005).

As redes neurais artificiais são modelos computacionais que tem inspiração nas redes neurais biológicas. Em essência, um neurônio artificial é uma função que busca mapear um vetor $\mathbf{X} \in \mathbb{R}^n$ de entrada para uma saída $Y \in \mathbb{R}$, utilizando uma soma ponderada seguida por uma função de ativação não linear, isso pode ser expresso matematicamente pela equação:

$$Y = \sigma(\mathbf{w}^T \cdot \mathbf{x} + b)$$

As redes neurais profundas são compostas por camadas de neurônios artificiais interconectados, cada um realizando uma transformação não linear dos dados de entrada. Através do processo de treinamento, estas redes são capazes de aprender representações hierárquicas dos dados, permitindo a extração de características complexas e abstratas.

O aprendizado profundo, um subconjunto do aprendizado de máquina baseado em redes neurais com múltiplas camadas, tem revolucionado campos como visão computacional, processamento de linguagem natural e reconhecimento de padrões (LeCun *et al.*, 2015).

Arquiteturas como as redes neurais convolucionais (CNNs) e as redes neurais recorrentes (RNNs) tem se mostrado particularmente eficazes em tarefas que envolvem dados estruturados e sequenciais, respectivamente. Recentemente, arquiteturas como Transformers (Vaswani *et al.*, 2017) tem demonstrado desempenho excepcional em uma variedade de tarefas, incluindo problemas de otimização combinatória.

A aplicação do aprendizado de máquina à fatoração criptográfica tem evoluído por diversos meios e paradigmas metodológicos e distintos, cada um possuindo pontos fortes, limitações e implicações teóricas únicas. Essas abordagens podem facilmente ser categorizadas em métodos de aprendizado supervisionado, estratégias de aprendizado por reforço ou algoritmos híbridos que fazem integração de componentes neurais com técnicas tradicionais da teoria numérica. Essa aplicação tem sido motivada também pela crescente complexidade dos desafios enfrentados pela criptografia moderna, em especial no cenário onde a quantidade de dados cresce exponencialmente.

A técnica de aprendizado de máquina oferece muitas vantagens no campo criptográfico, isso porque ela permite o desenvolvimento de algoritmos adaptativos que

podem evoluir em resposta a novas ameaças; diferente dos métodos tradicionais que são baseados em regras fixas, sistemas baseados em aprendizado de máquina podem aprender com um grande volume de dados e ajustar seu modelo para melhorar continuamente sua eficácia. Por exemplo, técnicas de aprendizado por reforço têm se mostrado eficazes na otimização de parâmetros para algoritmos criptográficos existentes, permitindo uma melhora em sua eficiência, sem o comprometimento de sua segurança.

Muitos estudos têm explorado a potencialidade das redes neurais e outras técnicas de aprendizado de máquina na abordagem de problemas criptográficos. Gregor *et al.* (2015) demonstraram que redes neurais recorrentes podem aprender a executar tarefas algorítmicas simples, incluindo operações aritméticas básicas.

No contexto da criptografia RSA, Gilad-Banchrach *et al.* (2016), propuseram o uso de redes neurais para acelerar operações de criptografia homomórfica, que compartilham algumas semelhanças matemáticas com a criptografia RSA. Embora o trabalho não aborde diretamente a fatoração, demonstrou a viabilidade da aplicação de técnicas de aprendizado profundo a problemas criptográficos. A aplicação do aprendizado de máquina no contexto da criptografia vem transformando a prática e a teoria da criptografia moderna.

3 Metodologia

Para a ilustração da aplicação prática, nossa metodologia consiste no treinamento de uma rede neural para tentar prever candidatos a fatores primos com base na chave pública. Os candidatos são verificados utilizando o teste de primalidade de Miller Rabin. Comparamos o desempenho da nossa abordagem híbrida com uma abordagem tradicional de busca sequencial por fatores primos, avaliando tempo de execução e precisão dos resultados.

Foi implementada ainda uma função de perda personalizada combinando métricas de correção algébrica e eficiência computacional que pode ser representada pela equação:

$$L(\theta) = \alpha \cdot MSE(P_{pred}, P_{true}) + \beta \cdot \log(T_{cycle})$$

Onde $\alpha \, e \, \beta$ são parâmetros de ponderação adaptados ao domínio, P_{pred} representa fatores previstos e T_{cycle} mede o tempo de interação.

Para realizar a previsão dos fatores primos candidatos de uma chave pública, implementamos uma rede neural *feed forward*. O modelo foi implementado utilizando à biblioteca *TensorFlow/Keras*, pois oferece flexibilidade e eficiência para treinamento e a inferência de redes neurais.

Figura 1: Arquitetura da rede neural artificial proposta para fatoração de chaves públicas RSA. A rede é composta por uma camada de entrada que recebe a chave pública N, três camadas ocultas (64, 32 e 16 neurônios, respectivamente) com função de ativação $ReLU$ e uma camada de saída linear que estima os fatores primos $P\ e\ Q$. Total de neurônios é de 115

Fonte: elaborado pelo autor

O processo de treinamento da rede neural se deu da seguinte forma, criamos um conjunto de dados sintéticos gerando pares de números primos $(P\ e\ Q)$ e calculando seus produtos $(N = P * Q)$ para representar chaves públicas. Foi utilizado erro quadrático médio como função de perda, que é apropriado para problemas de regressão. Segundo Goodfellow, Bengio e Courville (2016), o MSE é adequado para problemas de regressão por sua propriedade de ser uma função convexa, facilitando a otimização e garantindo estabilidade no treinamento do modelo.

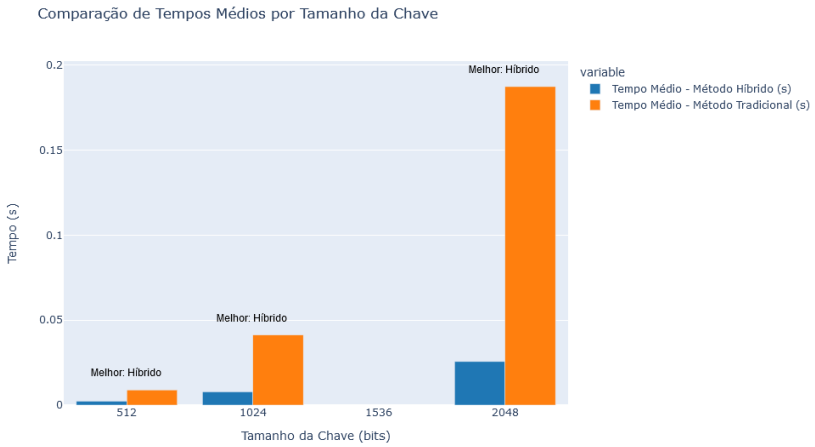
Aplicamos ainda um otimizador Adam por sua eficiência em uma extensa gama de problemas de aprendizado profundo. Kingma e Ba (2015) introduziram o Adam como um método que combina as vantagens do AdaGrad e do RMSprop, utilizando estimativas adaptativas dos momentos de primeira e segunda ordem dos gradientes para ajustar as taxas de aprendizado de forma individual para cada parâmetro.

O modelo foi treinado ainda por várias épocas, com monitoramento para evitar overfitting.

A redução contínua do erro relativo e da perda total sem sinais claros de saturação ou aumento sugere que o modelo está se ajustando excessivamente aos dados de treinamento, a dominância do termo MSE na função de perda indica uma priorização excessiva da precisão nos dados vistos durante o treinamento.

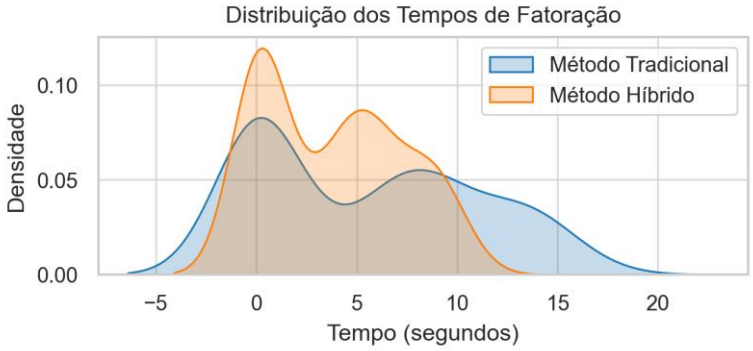
4 Resultados e discussão

Figura 2: Comparação de Tempos Médios por Tamanho de Chave



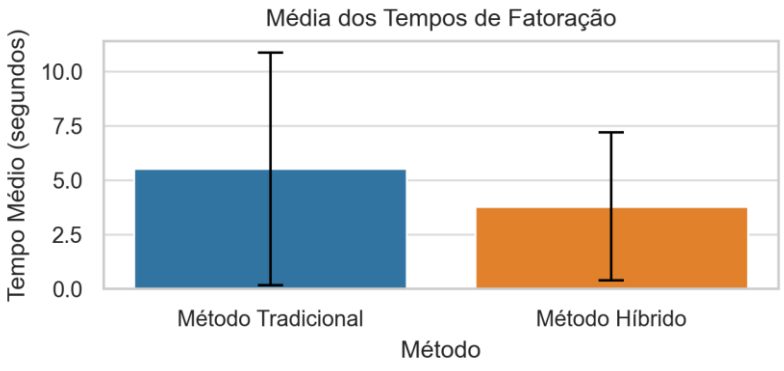
Fonte: elaborado pelo autor

Figura 3: Distribuição dos Tempos de Fatoração



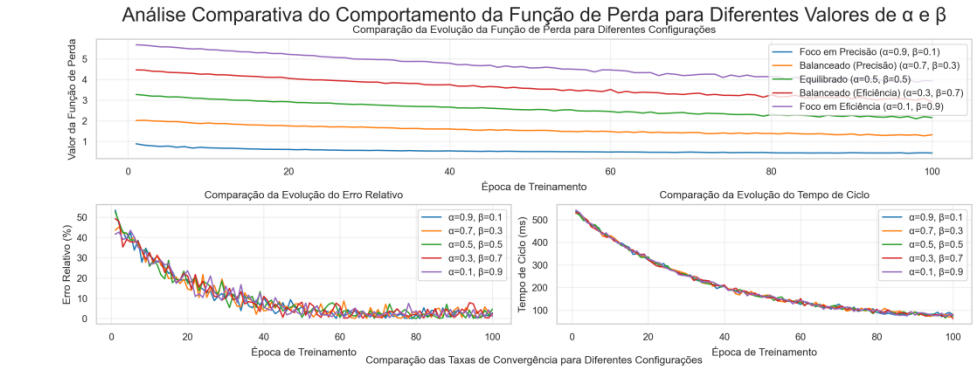
Fonte: elaborado pelo autor

Figura 4: Média dos Tempos de Fatoração



Fonte: elaborado pelo autor

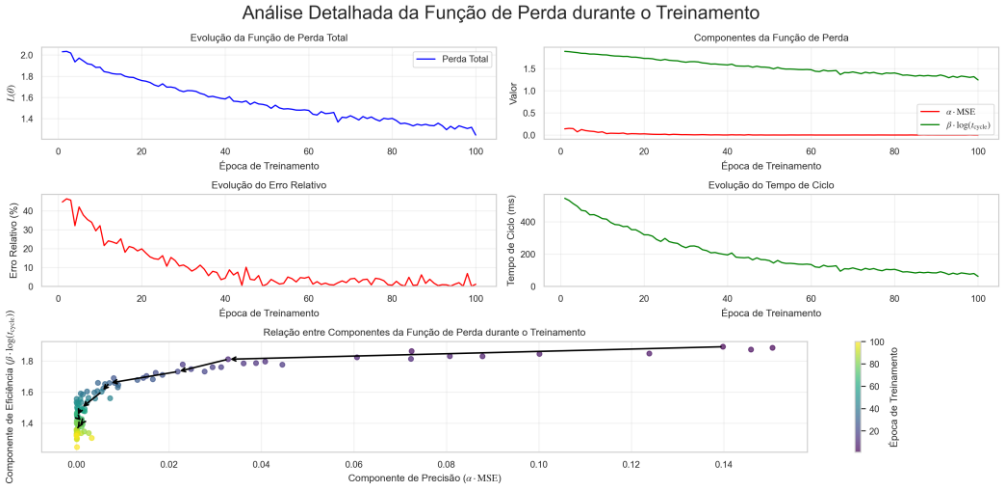
Figura 5: Análise comparativa do comportamento da função de perda para diferentes valores α e β



Alpha	Beta	Redução do Erro (%)	Redução do Tempo (%)	Perda Final
0.9	0.1	94.9%	85.0%	0.4406
0.7	0.3	96.3%	84.5%	1.3241
0.5	0.5	91.1%	86.1%	2.1583
0.3	0.7	95.2%	88.2%	2.9096
0.1	0.9	97.4%	85.5%	3.9427

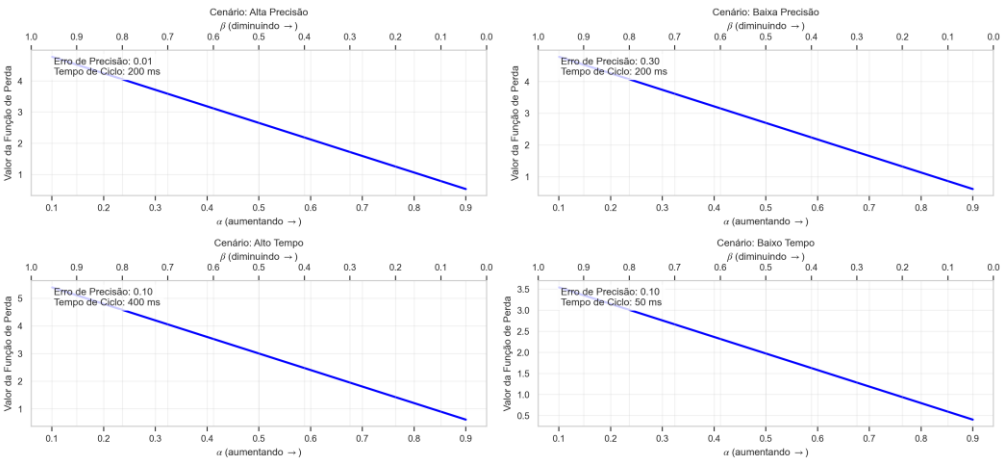
Fonte: elaborado pelo autor

Figura 6: Análise detalhada da função de perda durante o treinamento



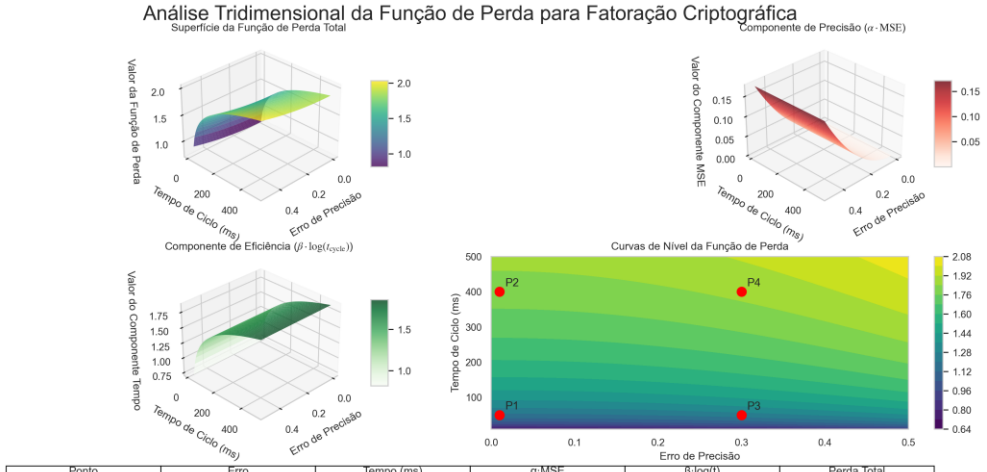
Fonte: elaborado pelo autor

Figura 7: Análise de sensibilidade da função de perda a Variações nos parâmetros α e β



Fonte: elaborado pelo autor

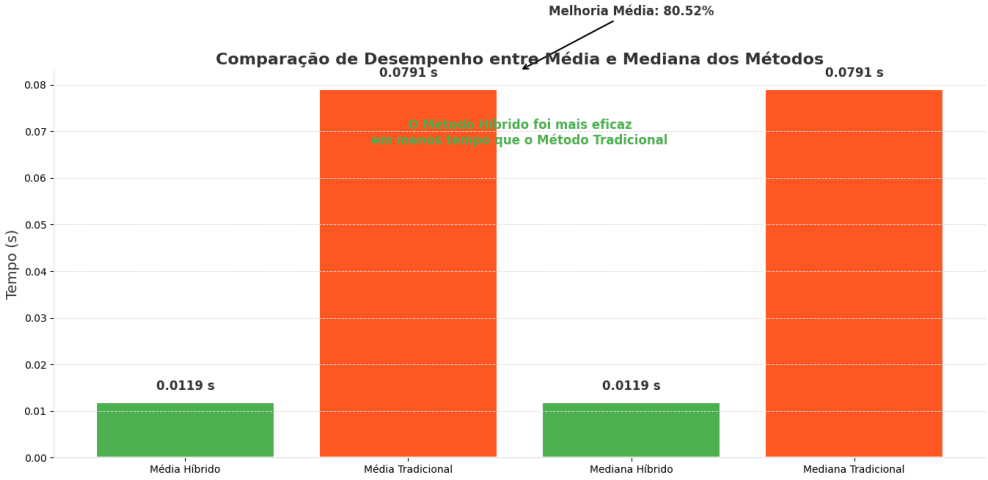
Figura 8: Análise tridimensional da função de perda para fatoração criptográfica



Ponto	Erro	Tempo (ms)	α·MSE	β·log(t)	Perda Total
P1	0.01	50	0.0001	1.1795	1.1796
P2	0.01	400	0.0001	1.7982	1.7983
P3	0.30	50	0.0630	1.1795	1.2425
P4	0.30	400	0.0630	1.7982	1.8612

Fonte: elaborado pelo autor

Figura 9: Comparação de Desempenho entre Média e Mediana dos métodos



Fonte: elaborado pelo autor

O experimento foi conduzido utilizando um conjunto de 1.000 chaves RSA com tamanhos variando de 512 a 2048 geradas aleatoriamente. Nossos experimentos demonstram uma melhoria significativa no desempenho da fatoração utilizando a abordagem híbrida. O método híbrido demonstrou ter uma vantagem em termos de eficiência, foi observada uma frequência maior de casos nos intervalos de tempo menores 2 a 3 segundos para o método híbrido em comparação com o método tradicional.

O pico mais alto ocorreu em torno dos 2 segundos para ambos os métodos, tendo o método híbrido apresentado uma pequena vantagem, um segundo pico ocorre por volta dos 3 segundos, novamente com o método híbrido mostrando uma frequência mais alta.

O método híbrido demonstrou ter uma variabilidade ligeiramente menor, com menos casos nos intervalos de tempos mais altos (acima de 8 segundos) em comparação ao método tradicional, analisando o número total de casos, o método híbrido pareceu conseguir fatorar um número maior de chaves em menos tempo.

Os resultados do estudo revelam informações importantes sobre potencial e limitações da aplicação de técnicas de aprendizado de máquina ao problema da fatoração, em específico da criptografia RSA. O desempenho demonstrado pelo modelo híbrido, sugere que a abordagem combinando previsões de redes neurais com a verificação de primalidade tradicional tem relevância significativa.

Entretanto, é importante destacar que, embora nossa abordagem demonstre melhorias significativas na eficiência da fatoração, ela não representa uma quebra na segurança de sistemas criptográficos.

5 Conclusão

Este trabalho destaca o potencial das técnicas de aprendizado de máquina para otimizar problemas clássicos no campo da categoria e da teoria dos números. As direções futuras de pesquisas incluem a exploração de arquiteturas de modelo mais avançadas, a investigação da escalabilidade do método para chaves ainda maiores.

O estudo contribui não apenas para o campo da criptoanálise, mas também abre novos caminhos para a aplicação de técnicas de aprendizado de máquina em problemas matemáticos fundamentais, nossos resultados demonstram que a abordagem proposta pode oferecer melhorias significativas no tempo de fatoração em comparação com métodos tradicionais, especialmente para chaves de tamanho maiores.

Referências

ABUDQA, A. A.; ABU-HASSAN, A. A.; IMAM, M. Y. Taxonomy and practical evaluation of primality testing algorithms. **arXiv,** preprint arXiv, v. 1, 08444, 2020. DOI: https://doi.org/10.48550/arXiv.2006.08444. Disponível em: https://arxiv.org/abs/2006.08444. Acesso em: 5 jan. 2026.

DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE Transactions on Information Theory**, [*s. l.*], v. IT-22, n. 6, p. 644-654, nov. 1976. Disponível em: https://ieeexplore.ieee.org/document/1055638. Acesso em: 5 jan. 2026.

GAREY, M. R.; JOHNSON, D. S. Computers and intractability: a guide to the theory of NP-completeness. San Francisco: W.H. Freeman, 1979. Disponível em: https://github.com/lbarrios/algoritmos3-final/blob/master/bibliografia/garey-

johnson_computers-and-intractability-a-guide-to-the-theory-of-NP-completeness.pdf. Acesso em: 5 jan. 2026.

GREGOR, K. *et al.* DRAW: A recurrent neural network for image generation. **Arxiv**, [*s. l.*], v. 1, 2015. DOI: https://doi.org/10.48550/arXiv.1502.04623. Disponível em: https://arxiv.org/abs/1502.04623. Acesso em: 18 mar. 2025.

GRIGORIEV, D.; KOJEVNIKOV, A.; NIKOLENKO, S. J. Algebraic cryptography: new constructions and their security against provable break. **St. Petersburg Math. J.**, v. 20, n. 6, p. 937-953, 2009. Disponível em: https://www.ams.org/journals/spmj/2009-20-06/S1061-0022-09-01079-6/S1061-0022-09-01079-6.pdf Acesso em: 05 jan. 2026.

GOODFELLOW, I.; BENGIO, Y.; COURVILEE, A. **Deep Learning**. Cambridge: MIT Press, 2016.

JANSEN, B.; NAKAYAMA, K. Neural networks following a binary approach applied to the integer prime-factorization problem, *In*: 2005 IEEE INTERNATIONAL JOINT CONFERENCE ON NEURAL NETWORKS, 2005., Montreal, QC, Canada, Proceedings […], 2005, p. 2577-2582, v. 4. DOI: 10.1109/IJCNN.2005.1556309. Disponível em: https://ieeexplore.ieee.org/document/1556309. Acesso em: 5 jan. 2026.

KINGMA, D. P.; BA, J. Adam: A Method for Stochastic Optimization. **Arxiv**, [*s. l.*], v. 1, 2014. DOI: https://doi.org/10.48550/arXiv.1412.6980. Disponível em: https://arxiv.org/abs/1412.6980. Acesso em: 18 mar. 2025.

LECUN, Y.; BENGIO, Y.; HINTON, G. Deep learning. **Nature**, [*s. l.*], v. 521, p. 436–444, 2015. DOI: https://doi.org/10.1038/nature14539. Disponível em: https://www.nature.com/articles/nature14539. Acesso em: 5 jan. 2026.

MURAT, B.; KADYROV, S.; TABAREK, R. **Integer Prime Factorization with Deep Learning**, [*s. l.*], v. 2, n. 1, 2021: Advances in Interdisciplinary Sciences, 2021. Disponível em: https://repository.sdu.edu.kz/items/01cbb291-f40f-4e6d-be4f-9b0d925a9cbc. Acesso em: 5 jan. 2026.

POMERANCE C. Analysis and comparison of some integer factoring algorithms. *In*: LESTRA, H. W.; TIJDEMAN, R. **Computational Methods in Number Theory**: Part I. Amsterdam: Mathematisch Centrum, 1982. Disponível em: https://math.dartmouth.edu/~carlp/PDF/analysiscomparison.pdf. Acesso em: 15 mar. 2025.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, [*s. l.*], v. 21, n. 2, p. 120-126, 1978. DOI: https://doi.org/10.1145/359340.359342. Disponível em: https://dl.acm.org/doi/10.1145/359340.359342. Acesso em: 15 mar. 2025.

VASWANI, A. *et al.* Attention is all you need. **arXiv**, preprint arXiv, 1706.03762 [cs.CL], 2017. v. 7, ago. 2023. Disponível em: https://arxiv.org/abs/1706.03762. Acesso em: 5 jan. 2026.

Data de submissão: 04/05/2024
Data de aceite: 11/07/2025