REVISTA DA MICRO E PEQUENA EMPRESA
Vol. 19, No. 3, Set-Dez 2025, p.75-95
ISSN: 1982-2537

CriptoÁrvore: análise de uma ferramenta visual para o ensino de criptografia e estruturas de dados*

CriptoÁrvore: analysis of a visual tool for teaching cryptography and data structures

Ricardo Alexandre Silva Galvão Filho
Universidade de Vassouras
pattz.rg@hotmail.com

Daniel Daigo Sasagawa
Universidade de Vassouras
daniel.daigo@gmail.com

Cauan Ferreira de Almeida
Universidade de Vassouras
cauanferreiraalmeida@gmail.com

Victor Ângelo Bastos Ferreira
Universidade de Vassouras
ferreira.victorbf@gmail.com

Fabricio Tadeu Dias
Universidade Federal Fluminense
fabricio_dias@id.uff.br

Marcio Alexandre Dias Garrido
Universidade Federal Fluminense
marciogarrido@id.uff.br

RESUMO

Este estudo analisa o CriptoÁrvore, ferramenta visual que integra criptografia, estruturas de dados e visualização interativa como recurso potencial para o ensino de segurança da informação. Adotou-se abordagem qualitativa, de natureza bibliográfica e documental, complementada pela análise técnica do código-fonte e da documentação do projeto. Desenvolvida em Python 3.12, a aplicação organiza seu fluxo em cinco camadas descritas na documentação: geração de chave baseada em SHA-256, salt aleatório, embaralhamento determinístico, proteção de chave por RSA-2048 e verificação de integridade, utilizando uma árvore binária para representação gráfica dos dados. Os testes documentados indicaram funcionamento consistente das operações de cifragem e decifragem e ausência de sucesso nas tentativas de criptoanálise realizadas no contexto avaliativo analisado. Os resultados caracterizam a ferramenta como uma proposta tecnológica com potencial educacional, embora sua eficácia pedagógica e segurança criptográfica não tenham sido mensuradas por protocolos específicos.

Palavras-chave: Segurança da informação. Árvore binária. Criptografia. Transformação digital. Capacitação profissional.

* Recebido em 30 de julho de 2025, aprovado em 30 de outubro de 2025, publicado em 30 de dezembro de 2025.

ABSTRACT

This study analyzes CriptoÁrvore, a visual tool that integrates cryptography, data structures, and interactive visualization as a potential resource for information security education. A qualitative approach was adopted, based on bibliographic and documentary research, complemented by a technical analysis of the project's source code and documentation. Developed in Python 3.12, the application organizes its processing workflow into five layers described in the documentation: SHA-256-based key generation, random salting, deterministic shuffling, RSA-2048 key protection, and integrity verification, using a binary tree for graphical data representation. The documented tests indicated consistent performance of the encryption and decryption operations and no successful cryptanalysis attempts within the evaluated context. The results characterize the tool as a technological proposal with educational potential, although its pedagogical effectiveness and cryptographic security were not assessed through specific evaluation protocols.

Keywords: Information security. Binary tree. Cryptography. Digital transformation. Professional training.

1. INTRODUÇÃO

A cibersegurança ocupa posição relevante na sociedade digital, uma vez que mecanismos de proteção da informação estão presentes em diferentes atividades mediadas por sistemas computacionais e redes de comunicação. A formação de estudantes em conceitos de segurança da informação e criptografia constitui, por isso, uma dimensão importante da preparação de profissionais de computação. A literatura sobre ensino de criptografia evidencia, entretanto, que o tema pode ser percebido como difícil pelos estudantes e que a motivação para a aprendizagem constitui um dos desafios associados ao seu ensino (MARIN; SOUZA; MARIN, 2021).

A dificuldade pedagógica não decorre exclusivamente da complexidade técnica dos algoritmos. Conceitos como funções hash, chaves criptográficas, operações modulares e mecanismos de autenticação exigem que o estudante articule diferentes níveis de abstração. Por esse motivo, recursos capazes de relacionar conceitos teóricos a representações e atividades concretas podem contribuir para a exploração didática do conteúdo. Marin, Souza e Marin (2021), por exemplo, investigaram o ensino de conceitos básicos de criptografia com estudantes do ensino médio profissional e utilizaram um instrumento de survey para analisar aspectos relacionados à motivação, compreensão e utilização de ferramentas computacionais. Os autores identificaram que a maioria dos estudantes considerava o tema de difícil aprendizagem, embora os participantes tenham conseguido praticar e aprender pelo menos uma das técnicas abordadas.

Estudos recentes também têm explorado abordagens interativas e lúdicas para o ensino de cibersegurança. O trabalho Cyber Defender, por exemplo, apresenta o desenvolvimento e a avaliação de um jogo educativo para o ensino de segurança cibernética e emprega diferentes instrumentos de avaliação para examinar aspectos como usabilidade, experiência do jogador, aspectos pedagógicos e potencial de aprendizagem (SANTOS et al., 2025). De forma complementar, o CriptoData propõe uma abordagem de ensino de criptografia por meio de computação desplugada (SILVA; GUARDA, 2019). Essas experiências indicam que recursos interativos constituem uma linha de investigação pertinente, embora a efetividade pedagógica de cada ferramenta dependa de avaliação específica.

O projeto CriptoÁrvore é analisado neste estudo como uma proposta que aproxima criptografia e estruturas de dados por meio de visualização. A ferramenta utiliza uma árvore binária para representar os dados durante o fluxo de transformação e disponibiliza uma interface gráfica destinada a tornar observáveis as diferentes etapas do processamento. A proposta não consiste na criação de um novo algoritmo criptográfico, mas na integração, em uma aplicação educacional, de mecanismos criptográficos e de uma estrutura de dados tradicional da Computação.

A preocupação com segurança também alcança sistemas de menor porte. Em aplicações desenvolvidas sob restrições técnicas, financeiras e organizacionais, a adoção de mecanismos de proteção desde a concepção do software constitui uma questão relevante (PEDRINI; CARVALHO, 2025). No âmbito das organizações de menor porte, a transformação digital também pode ser condicionada por fatores relacionados a competências, recursos e segurança, o que reforça a importância de abordagens que aproximem formação técnica e aplicação prática (BATISTA; AROUCA; LOBATO, 2024; COSTA et al., 2025). Essa perspectiva é particularmente pertinente para uma ferramenta educacional que procura relacionar conhecimentos de segurança computacional a fundamentos de desenvolvimento de software.

A análise também considera que a segurança de uma aplicação não deve ser caracterizada apenas pela presença de determinados algoritmos. A arquitetura, o modelo de ameaça, a forma de utilização das primitivas e a configuração efetivamente implementada são elementos relevantes para uma avaliação técnica (OWASP FOUNDATION, 2023a). O presente estudo evita, por isso, interpretar automaticamente cada transformação existente no CriptoÁrvore como uma primitiva criptográfica ou como uma garantia de segurança independente.

Adotou-se abordagem qualitativa, de natureza bibliográfica e documental, complementada por análise técnica dos artefatos do projeto. A pesquisa bibliográfica foi utilizada para contextualizar os fundamentos de criptografia, estruturas de dados, ensino de segurança computacional e segurança de software. A pesquisa documental concentrou-se na documentação e no código-fonte disponibilizados para análise, buscando identificar os componentes arquiteturais, o fluxo de transformação dos dados e as funcionalidades observáveis da aplicação.

O objetivo geral é analisar o projeto CriptoÁrvore, com foco em sua arquitetura criptográfica, na implementação e representação de estruturas de dados e em seu potencial de utilização como recurso educacional. Como objetivos específicos, busca-se: (i) descrever a arquitetura de proteção apresentada pelo projeto; (ii) relacionar seus componentes a fundamentos e recomendações de segurança pertinentes; (iii) analisar a utilização da árvore binária como elemento de representação visual; e (iv) discutir os resultados funcionais documentados e as limitações da avaliação realizada.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Desafios pedagógicos no ensino de cibersegurança e criptografia

O ensino de criptografia apresenta desafios relacionados tanto à abstração dos conteúdos quanto à necessidade de estabelecer relações entre os conceitos estudados e situações concretas de aplicação. Marin, Souza e Marin (2021) observaram, em investigação realizada com estudantes do ensino médio profissional, que a criptografia era considerada um tema de difícil aprendizagem por parcela significativa dos participantes. O estudo também procurou avaliar motivação, compreensão e utilização de ferramentas computacionais, demonstrando a pertinência de investigar empiricamente a relação entre recursos didáticos e aprendizagem.

A literatura recente apresenta diferentes estratégias para lidar com essas dificuldades. Entre elas estão jogos educativos, atividades interativas e propostas baseadas em computação desplugada. O CriptoData, de Silva e Guarda (2019), constitui uma experiência voltada ao ensino de criptografia por meio de computação desplugada. Já o Cyber Defender foi concebido como jogo educativo para o ensino de conceitos fundamentais de segurança digital e realizou avaliação específica de aspectos de usabilidade, experiência e potencial educacional (SANTOS et al., 2025).

Essas experiências permitem afirmar que estratégias interativas constituem objeto de investigação no ensino de segurança computacional, mas não permitem pressupor que qualquer ferramenta visual ou gamificada seja necessariamente eficaz. A eficácia pedagógica depende de objetivos de aprendizagem claramente definidos e de procedimentos de avaliação capazes de produzir evidências sobre aprendizagem, experiência ou desempenho. Essa distinção é importante para o CriptoÁrvore, uma vez que o presente estudo analisa a ferramenta e seus resultados funcionais, mas não realizou uma avaliação educacional específica com instrumentos de aprendizagem ou usabilidade.

A proposta do CriptoÁrvore aproxima esse debate do ensino de estruturas de dados. Árvores constituem estruturas hierárquicas utilizadas em diferentes algoritmos e aplicações computacionais, e sua representação gráfica pode auxiliar na observação da organização dos dados e das operações realizadas sobre seus nós (CORMEN et al., 2009). No projeto analisado, essa estrutura é utilizada em conjunto com transformações criptográficas, permitindo que o processamento seja apresentado por meio de uma representação visual.

2.2 Segurança de software e arquitetura de proteção

A análise da arquitetura de segurança deve considerar a finalidade de cada mecanismo e a forma como ele é integrado ao restante da aplicação, e não apenas os algoritmos empregados. A OWASP recomenda que decisões relacionadas à proteção de dados sejam precedidas pela consideração da arquitetura e do modelo de ameaça da aplicação. Também destaca a importância da utilização de primitivas criptográficas padronizadas, evitando mecanismos criptográficos personalizados sem fundamentação adequada (OWASP FOUNDATION, 2023a).

Essa perspectiva é relevante para o CriptoÁrvore porque sua arquitetura combina diferentes transformações. Algumas delas são diretamente associadas a primitivas criptográficas padronizadas, enquanto outras constituem operações de transformação realizadas pelo próprio fluxo da aplicação. Assim, o presente estudo distingue mecanismos criptográficos de transformações auxiliares e evita atribuir propriedades de segurança que não estejam demonstradas pela documentação ou por análise específica.

A preocupação com segurança desde a concepção também encontra correspondência na literatura sobre sistemas de pequeno porte. Pedrini e Carvalho (2025) discutem diretrizes relacionadas à aplicação da LGPD em sistemas de software de pequeno porte, considerando

restrições técnicas, financeiras e organizacionais. Embora o CriptoÁrvore tenha finalidade educacional e não constitua um sistema empresarial submetido à LGPD no escopo desta pesquisa, essa literatura contribui para contextualizar a importância de decisões de segurança proporcionais ao contexto de desenvolvimento.

Em contextos organizacionais marcados pela necessidade de inovação, iniciativas estruturadas de orientação e desenvolvimento podem apresentar potencial para geração de vantagem competitiva, especialmente quando associadas à implementação de práticas capazes de produzir valor para as organizações (ALVES; AIRES; SALGADO, 2023).

2.2.1 Funções hash e SHA-256

O projeto utiliza o SHA-256 em componentes descritos na documentação como geração de chave dinâmica e verificação de integridade. O SHA-256 integra a família SHA-2 especificada pelo National Institute of Standards and Technology (NIST) no FIPS 180-4 (NIST, 2015). Funções hash criptográficas recebem uma entrada de tamanho variável e produzem um resumo de tamanho fixo. No caso do SHA-256, o resumo possui 256 bits.

De forma simplificada, dada uma mensagem M, a função hash H pode ser representada por:

$$h=H(M)$$

Entre as propriedades criptográficas relevantes das funções hash estão a resistência à preimagem, à segunda preimagem e às colisões. No caso da resistência à colisão, busca-se tornar computacionalmente inviável encontrar duas entradas distintas M e M′ que produzam o mesmo resumo:

$$H(M)=H(M'),M\neq M'$$

Essa propriedade contribui para a utilização de funções hash em mecanismos de detecção de alterações, mas não deve ser confundida com autenticação da mensagem. Um valor SHA-256 calculado isoladamente permite comparar resumos quando existe um valor de referência confiável; entretanto, se um adversário puder modificar simultaneamente a mensagem e o resumo utilizado na comparação, o hash, por si só, não fornece autenticação contra esse adversário. Para essa finalidade, podem ser utilizados mecanismos adicionais, como códigos de autenticação de mensagens baseados em chave ou assinaturas digitais, conforme o modelo de segurança adotado.

No CriptoÁrvore, portanto, o SHA-256 é analisado como função de resumo e como componente do fluxo documentado de geração e verificação. A propriedade efetivamente proporcionada pela etapa de verificação de integridade depende, contudo, da forma como o valor produzido é armazenado, transmitido e protegido contra substituição. Essa informação precisa ser considerada na análise da implementação concreta.

2.2.2 Salt e transformação dos dados

A documentação do CriptoÁrvore descreve a utilização de um salt aleatório como uma das etapas do fluxo de transformação. Em termos gerais, um salt é um valor adicional utilizado juntamente com uma entrada antes de determinada operação criptográfica. Uma representação simplificada da combinação de uma mensagem M com um salt S pode ser expressa por:

$$h' = H(M \| S)$$

em que ‖ representa a concatenação dos valores.

No contexto de armazenamento de senhas, a utilização de salts únicos é uma prática estabelecida para impedir que entradas iguais produzam diretamente os mesmos valores armazenados e para dificultar o aproveitamento de tabelas pré-computadas. A OWASP trata essa aplicação do salt especificamente no contexto de armazenamento de senhas e recomenda, para essa finalidade, funções de derivação de chave apropriadas, como Argon2id, bcrypt ou PBKDF2 (OWASP FOUNDATION, 2023b).

Essa finalidade não deve ser transferida automaticamente para qualquer arquitetura de criptografia de mensagens. No caso do CriptoÁrvore, embora a documentação registre a presença de um salt aleatório, o material analisado não apresenta informações suficientes para caracterizar essa etapa como uma função de derivação de chave nem para estabelecer, com precisão, os parâmetros de uma eventual KDF. Também não é possível concluir, apenas pela presença do salt, que a operação efetivamente implementada corresponda à forma simplificada H(M‖S) apresentada acima.

Por essa razão, a equação é utilizada neste artigo como representação conceitual da combinação entre uma entrada e um salt, e não como especificação da implementação do CriptoÁrvore. No projeto analisado, o salt é tratado como componente do fluxo de transformação documentado. Uma avaliação criptográfica mais aprofundada deverá identificar

a entrada à qual o salt é aplicado, sua relação com a geração ou derivação de chaves, seus parâmetros e sua finalidade efetiva.

2.2.3 Criptografia assimétrica e RSA-2048

O CriptoÁrvore utiliza RSA-2048 como componente assimétrico de sua arquitetura. O RSA utiliza um par de chaves, pública e privada, cuja construção está relacionada à aritmética modular. De forma simplificada, a geração do módulo N parte de dois números primos p e q:

$$N=p\times q$$

A função totiente de Euler, em sua formulação correspondente a esse caso, pode ser representada por:

$$\varphi(N)=(p-1)(q-1)$$

A partir desses valores são estabelecidos parâmetros relacionados às chaves pública e privada. Em uma representação simplificada da operação RSA, a transformação de uma mensagem representada por K, utilizando a chave pública (e,N), pode ser expressa como:

$$C=K^{e}\ (mod\ N)$$

e a operação inversa, utilizando o expoente privado d, pode ser representada por:

$$K=C^{d}\ (mod\ N)$$

Essas equações apresentam o princípio matemático básico do RSA, mas não constituem, isoladamente, uma especificação segura de uma implementação concreta. Em aplicações reais, a segurança depende também do esquema de codificação e preenchimento empregado, dos parâmetros utilizados, da geração e proteção das chaves e da finalidade específica da operação. Assim, a representação matemática acima não deve ser interpretada como descrição completa do mecanismo efetivamente utilizado pelo CriptoÁrvore.

A documentação analisada descreve uma arquitetura na qual uma chave utilizada no processamento dos dados é protegida por RSA, enquanto os dados propriamente ditos são processados por mecanismo simétrico. Esse arranjo corresponde ao princípio geral de uma arquitetura híbrida, na qual a criptografia simétrica é utilizada para o processamento de dados e um mecanismo assimétrico é empregado para proteger ou estabelecer o segredo utilizado nessa etapa.

Entretanto, a implementação concreta de uma arquitetura híbrida depende da especificação do algoritmo simétrico, do tamanho da chave, do modo de operação, do tratamento de IVs ou nonces, do mecanismo de autenticação e do esquema de padding empregado pelo RSA. No material analisado, esses elementos não estão suficientemente documentados para que possam ser especificados com segurança neste artigo.

Para RSA utilizado em criptografia, recomendações técnicas como as da OWASP ressaltam a importância de esquemas de padding adequados, incluindo OAEP em situações aplicáveis (OWASP FOUNDATION, 2023a). Embora o projeto documente o emprego de RSA-2048, o presente estudo não atribui à implementação um esquema de padding específico sem evidência documental. A ausência dessa informação constitui uma limitação da caracterização técnica e indica um ponto a ser detalhado em documentação futura ou em uma avaliação posterior da implementação.

2.3 Estruturas de dados e representação visual

Estruturas de dados constituem mecanismos fundamentais para organização e manipulação de informações em algoritmos. Árvores binárias permitem representar relações hierárquicas entre elementos e constituem uma estrutura tradicionalmente estudada em disciplinas de algoritmos e estruturas de dados (CORMEN et al., 2009).

No CriptoÁrvore, a árvore binária assume também uma função de representação. A interface gráfica permite observar os dados organizados em nós e acompanhar visualmente o estado do processamento. Essa característica estabelece uma relação entre dois conteúdos que normalmente podem ser apresentados separadamente: a organização dos dados por estruturas hierárquicas e a transformação dos dados por mecanismos criptográficos.

A presença de uma representação visual, contudo, não constitui evidência suficiente para afirmar que houve melhoria de aprendizagem. Para demonstrar esse efeito seriam necessários procedimentos específicos de avaliação, como testes de conhecimento, medidas de desempenho, instrumentos de usabilidade ou comparação entre condições de ensino. O presente estudo não realizou esse tipo de mensuração.

3. METODOLOGIA

3.1 Caracterização da pesquisa

A pesquisa adotou abordagem qualitativa, de natureza bibliográfica e documental, complementada por análise técnica dos artefatos do projeto CriptoÁrvore. A pesquisa bibliográfica foi utilizada para fundamentar conceitos relacionados ao ensino de criptografia, estruturas de dados, segurança de software e mecanismos criptográficos. Foram consideradas referências acadêmicas e documentos técnicos de organismos reconhecidos, incluindo NIST e OWASP.

A pesquisa documental concentrou-se na documentação do projeto, em seus artefatos técnicos e no código-fonte disponibilizado para análise. O objetivo foi identificar os componentes da arquitetura, o fluxo das transformações, a representação dos dados e as funcionalidades observáveis da aplicação.

A classificação como pesquisa qualitativa evita caracterizar o estudo como pesquisa de métodos mistos ou como experimento científico. Embora o desenvolvimento do software tenha utilizado práticas ágeis e controle de versão por Git/GitHub, essas práticas descrevem o processo de desenvolvimento e não constituem, isoladamente, um desenho experimental.

3.2 Procedimento de análise dos artefatos

A análise técnica foi organizada em quatro categorias:

- arquitetura de segurança: identificação das camadas e dos mecanismos descritos na documentação;
- transformação dos dados: identificação das operações realizadas durante os processos de cifragem e decifragem;
- representação visual: análise da utilização da árvore binária e da interface gráfica;
- resultados funcionais documentados: análise das evidências relativas ao funcionamento das operações de cifragem, decifragem e aos testes acadêmicos de criptoanálise descritos na documentação.

A análise considerou a documentação do projeto e o código-fonte disponibilizado. Entretanto, o material utilizado no presente estudo não registra de forma suficiente um protocolo formal de auditoria contendo, por exemplo, commit específico, data de coleta, conjunto completo de arquivos analisados e procedimento de codificação dos achados. Essa limitação impede apresentar a inspeção como uma auditoria criptográfica formal e deve ser considerada na interpretação dos resultados.

3.3 Desenvolvimento do software

Conforme a documentação do projeto, o CriptoÁrvore foi desenvolvido em Python 3.12, utilizando bibliotecas e recursos destinados à implementação criptográfica, construção da interface gráfica e visualização dos dados. Entre os componentes indicados estão a biblioteca Cryptography, Tkinter e Matplotlib.

O desenvolvimento foi conduzido com práticas ágeis e controle de versão por Git/GitHub, conforme os artefatos do projeto. Para fins desta pesquisa, entretanto, o processo de desenvolvimento foi tratado como contexto documental da aplicação, e não como experimento científico. Não foram definidos grupos experimentais, variáveis independentes e dependentes ou condições de comparação que permitissem caracterizar o desenvolvimento como experimento.

3.4 Arquitetura de cinco camadas

A documentação do CriptoÁrvore apresenta uma organização em cinco camadas de proteção e transformação. O Quadro 1 sintetiza essa organização, identificando a função de cada camada no fluxo de transformação sem atribuir, a priori, propriedades de segurança não demonstradas.

Quadro 1: Arquitetura de cinco camadas do CriptoÁrvore

Camada	Mecanismo descrito	Analogia utilizada no projeto	Função no fluxo
1	Chave dinâmica baseada em SHA-256	Impressão digital	Geração/transformação de chave conforme o fluxo documentado
2	Salt aleatório	Cardápio de códigos	Inclusão de aleatoriedade no fluxo de transformação
3	Embaralhamento determinístico	Quebra-cabeça	Reordenação determinística dos dados
4	Proteção RSA-2048	Cofre de banco	Proteção assimétrica da chave descrita na arquitetura
5	Verificação de integridade	Lacre de segurança	Verificação do valor de integridade previsto pelo fluxo

A denominação “função no fluxo”, em vez de “função de segurança”, é deliberada: o embaralhamento determinístico, por exemplo, constitui uma transformação dos dados, mas não deve ser considerado primitiva criptográfica apenas por dificultar visualmente a interpretação do conteúdo. Da mesma forma, a capacidade de uma etapa de fornecer integridade ou autenticidade depende de como seu resultado é protegido e verificado.

A interface gráfica centraliza as operações de cifragem e decifragem e apresenta ao usuário as etapas do processamento. A representação visual busca, dessa forma, tornar observáveis transformações que, em uma implementação exclusivamente textual, poderiam permanecer abstratas.

3.5 Critérios de interpretação dos resultados

Os resultados foram interpretados em duas dimensões distintas. A primeira corresponde ao funcionamento técnico observado, envolvendo as operações de cifragem e decifragem e os testes descritos na documentação. A segunda corresponde ao potencial educacional da proposta, analisado a partir das características da ferramenta e de sua relação com a literatura.

Não se considerou que o funcionamento técnico, isoladamente, constituísse prova de eficácia pedagógica. Da mesma maneira, os testes realizados em contexto acadêmico não foram tratados como certificação ou validação formal da segurança criptográfica da aplicação.

Essa distinção é necessária porque avaliações educacionais e avaliações de segurança possuem objetivos e protocolos distintos. Enquanto a primeira requer evidências relacionadas à aprendizagem, experiência ou desempenho dos usuários, a segunda demanda a definição de um modelo de ameaça, hipóteses de ataque, condições experimentais, métricas e critérios de sucesso.

3.6 Limitações metodológicas

As principais limitações metodológicas identificadas foram a ausência de uma avaliação pedagógica específica, a inexistência de um protocolo formal de avaliação criptográfica e a insuficiência de informações documentais para caracterizar alguns parâmetros da implementação criptográfica.

Não foram coletados, neste estudo, dados de aprendizagem antes e depois da utilização da ferramenta, medidas de retenção, comparação com outra estratégia didática ou instrumentos padronizados de usabilidade. Também não foram apresentados no material analisado dados suficientes para especificar integralmente o algoritmo simétrico empregado, seus parâmetros, o esquema de padding utilizado no RSA ou o mecanismo exato de proteção do valor de integridade.

Essas limitações não invalidam a análise do projeto como estudo de caso, mas delimitam o alcance das conclusões. Os resultados devem ser entendidos como evidências sobre a

implementação e o funcionamento documentados, bem como sobre o potencial da proposta, e não como demonstração definitiva de eficácia pedagógica ou de segurança criptográfica geral

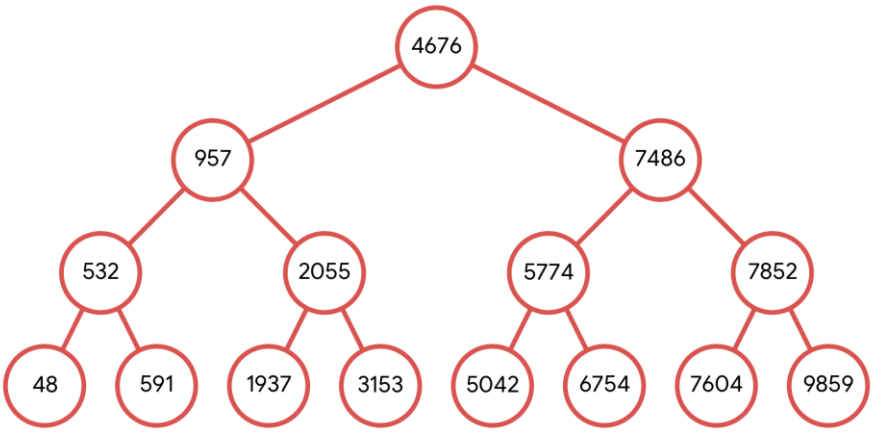
4. RESULTADOS E DISCUSSÃO

4.1 Resultados funcionais e visuais

De acordo com a documentação do projeto, o CriptoÁrvore foi capaz de realizar as operações de cifragem e decifragem previstas em sua arquitetura, permitindo recuperar os dados processados pelo fluxo implementado. Esse resultado constitui evidência de funcionamento das operações implementadas no contexto em que foram executadas.

O aspecto visual constitui uma das características centrais da proposta. A aplicação representa os dados por meio de uma árvore binária e utiliza a biblioteca Matplotlib para sua apresentação gráfica. A Figura 1 apresenta a representação da árvore no estado criptografado.

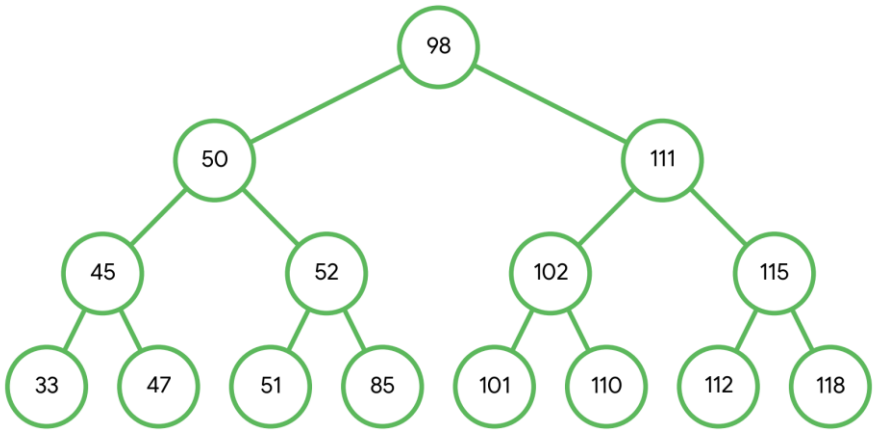
Figura 1: Visualização da árvore binária com dados criptografados



Fonte: Os autores.

A Figura 2 apresenta a representação correspondente após a decifragem.

Figura 2: Visualização da árvore binária com dados descriptografados



Fonte: Os autores.

A representação permite observar visualmente a estrutura dos dados antes e depois das operações realizadas pelo programa. Sob a perspectiva de estruturas de dados, essa característica aproxima a execução do software da representação gráfica de uma estrutura hierárquica, conceito tradicionalmente abordado no ensino de algoritmos e estruturas de dados (CORMEN et al., 2009).

Do ponto de vista pedagógico, entretanto, é necessário distinguir disponibilizar uma representação visual de demonstrar que essa representação produz aprendizagem superior. O presente estudo não realizou testes de aprendizagem, comparação entre grupos, avaliação de retenção ou instrumento específico de usabilidade. Assim, a visualização deve ser compreendida como um recurso concebido para tornar observáveis as transformações dos dados, e sua efetividade pedagógica permanece como questão para investigação posterior.

Essa delimitação é coerente com estudos que efetivamente realizam avaliações educacionais específicas. Marin, Souza e Marin (2021), por exemplo, utilizaram survey para investigar motivação, compreensão e utilização de ferramentas no ensino de criptografia. De modo semelhante, o estudo do Cyber Defender utilizou instrumentos específicos para avaliar usabilidade, experiência, aspectos pedagógicos e aprendizagem percebida (SANTOS et al., 2025). A diferença metodológica reforça por que o CriptoÁrvore, no estágio analisado, deve ser caracterizado como ferramenta com potencial educacional, e não como recurso cuja eficácia pedagógica já tenha sido comprovada.

4.2 Testes realizados no contexto avaliativo

Conforme a documentação do projeto, o CriptoÁrvore foi submetido a testes no contexto de uma atividade acadêmica na qual grupos de discentes realizaram tentativas de criptoanálise reversa sobre os pares participantes. Segundo os registros analisados, as tentativas realizadas nesse contexto não obtiveram sucesso em quebrar o fluxo de proteção implementado.

Esse resultado é relevante como evidência funcional dentro do contexto específico em que o software foi utilizado. Ele indica que, nas condições da atividade descrita na documentação, os participantes não conseguiram recuperar ou subverter a proteção implementada por meio das tentativas realizadas.

Entretanto, não é metodologicamente adequado transformar esse resultado em uma afirmação geral de resistência criptográfica. O material analisado não apresenta protocolo suficientemente detalhado quanto ao modelo de ameaça, aos recursos disponibilizados aos participantes, ao número de tentativas, ao tempo de execução, às ferramentas utilizadas, ao conhecimento prévio sobre a implementação, aos dados de entrada ou aos critérios formais de sucesso.

Por essa razão, evita-se aqui expressões como “testes rigorosos”, “vetores comuns de ataque”, “resistência notável” ou “validação irrefutável da eficácia”, que sugeririam um nível de comprovação não sustentado pelos dados disponíveis. O resultado é descrito, de forma mais precisa, como evidência funcional limitada ao contexto acadêmico documentado.

Essa distinção é particularmente importante porque segurança criptográfica não é uma propriedade estabelecida simplesmente pela ausência de sucesso em um conjunto não formalizado de tentativas. A análise de uma arquitetura de proteção deve considerar o modelo de ameaça e a utilização correta das primitivas criptográficas (OWASP FOUNDATION, 2023a). A própria OWASP recomenda que decisões arquiteturais relacionadas à proteção de dados sejam orientadas pela consideração dos adversários e das propriedades de segurança que se pretende alcançar.

4.3 Relação entre arquitetura e defesa em profundidade

A arquitetura de cinco camadas constitui uma característica relevante do projeto porque organiza diferentes operações em sequência. A documentação associa a cada camada uma função específica no fluxo, incluindo geração de chave, utilização de salt, embaralhamento, proteção assimétrica e verificação de integridade.

O conceito de defesa em profundidade é compatível, em termos arquiteturais, com a utilização de múltiplos controles, mas a simples multiplicação de transformações não implica necessariamente multiplicação equivalente da segurança. Para que cada camada contribua efetivamente para uma propriedade de segurança, é necessário conhecer sua finalidade, suas hipóteses, seus parâmetros e sua relação com as demais camadas.

A análise realizada permite afirmar que o CriptoÁrvore possui uma arquitetura multicamada documentada, mas não permite quantificar a contribuição individual de cada camada para a segurança global.

Essa distinção também é importante para o embaralhamento determinístico. A operação possui função no fluxo de transformação dos dados, mas não deve ser considerada uma primitiva criptográfica apenas porque altera a disposição das informações. Sua contribuição deve ser interpretada como transformação auxiliar, salvo demonstração específica de propriedade criptográfica sob determinado modelo de ameaça.

4.4 Discussão sobre SHA-256, integridade e autenticação

A utilização de SHA-256 no projeto é tecnicamente coerente com a existência de uma função de resumo criptográfico. O NIST especifica SHA-256 no âmbito do FIPS 180-4 e descreve funções hash como mecanismos para produzir resumos que podem ser utilizados para detectar alterações nas mensagens.

A interpretação da quinta camada, no entanto, exige precisão terminológica: integridade e autenticidade são propriedades relacionadas, mas não equivalentes. Um hash não autenticado pode permitir detectar uma alteração quando existe um valor de referência confiável e protegido, mas não impede que um adversário que possa substituir tanto a mensagem quanto o hash produza um novo par consistente.

A autenticação de mensagens requer mecanismos adicionais baseados em segredo compartilhado, como MAC/HMAC, ou mecanismos de assinatura digital, conforme o contexto. O NIST mantém recomendações específicas para códigos de autenticação de mensagens, enquanto suas referências sobre assinaturas digitais tratam da detecção de modificações e da autenticação da identidade do signatário (NIST, 2015; NIST, 2024).

Evita-se, por isso, afirmar que essa camada “garante que a mensagem não foi adulterada (autenticidade)”; descreve-se, de modo mais restrito, que a camada realiza a verificação do

valor de integridade previsto pelo fluxo da aplicação. A propriedade de autenticação somente pode ser atribuída se o mecanismo efetivamente utilizado para proteger esse valor for identificado e analisado.

4.5 Discussão sobre salt e transformação

A presença do salt deve ser interpretada de acordo com sua finalidade efetiva na implementação. A OWASP apresenta o salt principalmente no contexto de armazenamento de senhas, destacando sua função contra tabelas pré-computadas e sua necessidade de unicidade nesse cenário.

Como o CriptoÁrvore não é apresentado como um sistema de armazenamento de senhas, não é apropriado afirmar que a simples utilização de um salt produz, automaticamente, as mesmas propriedades descritas para password storage. A documentação analisada não fornece detalhes suficientes para determinar se o salt integra uma KDF, uma chave dinâmica ou outra transformação.

Essa limitação não elimina a relevância do componente no estudo. Pelo contrário, evidencia a necessidade de documentar de maneira mais precisa as entradas, saídas e finalidades de cada etapa de uma arquitetura criptográfica. Para uma futura versão técnica do projeto, recomenda-se especificar formalmente a finalidade do salt e sua relação com a geração ou derivação de chaves.

4.6 Discussão sobre RSA-2048 e arquitetura híbrida

A utilização de RSA-2048 é um dos elementos centrais da arquitetura descrita no projeto. O uso de mecanismos assimétricos para proteger um segredo empregado em uma etapa simétrica é uma estratégia conhecida em arquiteturas híbridas. Entretanto, a análise da segurança dessa construção exige especificar o mecanismo simétrico, seu modo de operação, o tratamento de IVs ou nonces, a forma de autenticação e o esquema de padding empregado pelo RSA.

A documentação disponibilizada para o presente estudo não apresenta todas essas informações. Por isso, o artigo mantém a descrição de RSA-2048 como componente da arquitetura, mas não afirma qual padding ou algoritmo simétrico específico foi empregado.

Essa ausência é uma limitação técnica importante. A OWASP recomenda a utilização de modos autenticados, como GCM ou CCM, quando disponíveis, e recomenda padding

aleatório/OAEP para operações de RSA utilizadas em criptografia. Entretanto, tais recomendações não autorizam concluir que essas configurações estejam presentes no CriptoÁrvore sem inspeção documental ou técnica que as comprove.

Consequentemente, uma avaliação futura deverá registrar explicitamente, para cada componente criptográfico, o algoritmo, tamanho de chave, modo de operação, parâmetros de aleatoriedade, mecanismo de autenticação e configuração de padding. Essa documentação aumentaria a reprodutibilidade da análise e permitiria uma avaliação de segurança mais precisa.

4.7 Discussão pedagógica

A principal contribuição potencial do CriptoÁrvore encontra-se na aproximação entre duas áreas tradicionalmente estudadas em componentes curriculares distintos: estruturas de dados e segurança da informação. A aplicação utiliza a árvore binária como elemento visual do processamento dos dados criptográficos, e não apenas como conteúdo abstrato.

Essa característica é compatível com a literatura que investiga recursos interativos para o ensino de criptografia e cibersegurança. Marin, Souza e Marin (2021) demonstram a existência de dificuldades percebidas pelos estudantes no aprendizado de criptografia, enquanto experiências como CriptoData e Cyber Defender exploram estratégias interativas ou lúdicas em contextos educacionais distintos (SILVA; GUARDA, 2019; SANTOS et al., 2025).

A contribuição específica do CriptoÁrvore está na combinação de visualização de uma estrutura de dados com um fluxo criptográfico. Em vez de apresentar a criptografia exclusivamente como uma sequência de operações matemáticas, o projeto procura associar a transformação dos dados à representação de uma árvore binária.

Os resultados do presente estudo são compatíveis com a hipótese de que esse tipo de visualização pode constituir recurso útil para exploração integrada dos conceitos. Contudo, essa hipótese não foi empiricamente testada. Não foram obtidos dados suficientes para afirmar que a ferramenta aumenta aprendizagem, motivação, retenção ou desempenho dos estudantes.

A distinção é importante para preservar a validade científica do estudo. O artigo analisa o potencial de uma ferramenta educacional; ele não apresenta uma avaliação experimental de sua eficácia pedagógica.

A relação entre segurança, desenvolvimento de software e organizações de menor porte constitui uma dimensão complementar da discussão. Estudos publicados na Revista da Micro e

Pequena Empresa apontam que limitações técnicas, financeiras e organizacionais podem influenciar a adoção de tecnologias e práticas de segurança em pequenos negócios (PEDRINI; CARVALHO, 2025; COSTA et al., 2025). A digitalização também envolve competências e condições organizacionais que podem afetar a capacidade de utilização dos recursos tecnológicos (BATISTA; AROUCA; LOBATO, 2024).

O CriptoÁrvore pode, nesse cenário, ser compreendido como uma proposta de formação técnica que aproxima conceitos de segurança de uma prática concreta de desenvolvimento. Sua contribuição para esse escopo não decorre de uma validação de uso empresarial, que não foi realizada, mas da possibilidade de utilizar um problema de desenvolvimento de software para discutir simultaneamente estruturas de dados e fundamentos de proteção da informação.

A literatura da própria Revista da Micro e Pequena Empresa também evidencia a importância de considerar aspectos humanos e organizacionais na segurança. Carvalho e Pedrini (2025), ao discutirem engenharia social em instituições de ensino superior, destacam que a segurança não depende exclusivamente de mecanismos tecnológicos, envolvendo também comportamento e conscientização. Embora o CriptoÁrvore tenha foco distinto, essa perspectiva reforça a importância de integrar formação técnica e compreensão dos mecanismos de segurança.

5. CONSIDERAÇÕES FINAIS

Este estudo alcançou o objetivo de analisar o CriptoÁrvore quanto à sua arquitetura de proteção, à utilização de estruturas de dados e ao potencial de aplicação educacional. A análise documental e técnica permitiu compreender a organização do software e seus principais componentes, bem como distinguir evidências de funcionamento daquelas que exigiriam avaliações específicas de segurança ou aprendizagem.

O principal achado foi que o CriptoÁrvore integra, em uma mesma experiência computacional, mecanismos criptográficos e a representação de dados por árvore binária, com funcionamento documentado das operações de cifragem e decifragem. As tentativas de criptoanálise realizadas no contexto acadêmico analisado também não resultaram na quebra do fluxo implementado. Esses resultados sustentam a caracterização da ferramenta como uma proposta funcional no contexto investigado, mas não como evidência de segurança criptográfica geral.

A principal contribuição do estudo está, portanto, na caracterização de uma abordagem que aproxima conteúdos de estruturas de dados e segurança da informação por meio de visualização interativa. A árvore binária deixa de atuar apenas como objeto de estudo e passa a compor a representação do processamento criptográfico, criando uma possibilidade de articulação entre conteúdos que tradicionalmente podem ser tratados de forma independente. Entretanto, o potencial educacional identificado permanece como uma hipótese fundamentada nas características da ferramenta, e não como eficácia pedagógica demonstrada empiricamente.

O alcance dos resultados é limitado pela ausência de avaliação educacional específica e de um protocolo formal de análise criptográfica. Não foram mensurados aprendizagem, retenção, usabilidade ou comparação com outras estratégias didáticas, tampouco foram suficientemente documentados alguns parâmetros da implementação, como o mecanismo simétrico empregado, o esquema de padding do RSA e a forma de proteção do valor utilizado na verificação de integridade. Essas lacunas impedem conclusões mais amplas sobre desempenho pedagógico e segurança da aplicação.

Estudos futuros devem avançar nessas duas frentes de forma complementar. No âmbito técnico, recomenda-se formalizar a documentação dos algoritmos, parâmetros e propriedades de segurança e conduzir uma avaliação baseada em modelo de ameaça, métricas e critérios de sucesso previamente definidos. No âmbito educacional, estudos com estudantes devem empregar instrumentos de aprendizagem, usabilidade e experiência, preferencialmente com delineamentos comparativos que permitam verificar os efeitos do uso da ferramenta. A partir desses resultados, extensões como comunicação entre participantes e investigação de mecanismos pós-quânticos poderão ser avaliadas com maior precisão e alinhamento às funções criptográficas efetivamente desempenhadas pelo sistema.

6. REFERÊNCIAS

ALVES, Ítalo Bruno Gomes; AIRES, Renan Felinto de Farias; SALGADO, Camila Cristina Rodrigues. O potencial de gerar vantagem competitiva de ações do programa Agentes Locais de Inovação (ALI): um estudo de caso em micro e pequenas empresas do Rio Grande do Norte. **Revista da Micro e Pequena Empresa**, v. 17, n. 1, p. 5-20, 2023. DOI: 10.6034/rmpe.v17i1.1507.

BATISTA, Alessandra Giselle Silva; AROUCA, Marcia Waimer Spinola; LOBATO, Fábio Manoel França. Estratégias de digitalização comunicacional para Micro e Pequenas Empresas como promotoras da inovação e competitividade. **Revista da Micro e Pequena Empresa**, v. 18, n. 3, p. 60-79, 2024. DOI: 10.6034/rmpe.v18i3.1982.

CARVALHO, Matheus Almeida de; PEDRINI, Júlio César Ferreira. Engenharia social no ambiente acadêmico: vulnerabilidade humana e estratégias de conscientização em instituições de ensino superior. **Revista da Micro e Pequena Empresa**, v. 19, n. 1, p. 139-154, 2025. DOI: 10.6034/rmpe.v19i1.2170.

CORMEN, Thomas H. et al. **Algoritmos: teoria e prática**. 3. ed. Rio de Janeiro: Elsevier, 2009.

COSTA, Leandro Loffeu Pereira; DIAS, Fabricio Tadeu; BARBOZA, Douglas Vieira; GARRIDO, Marcio Alexandre Dias. Propulsores e barreiras da virtualização em micro e pequenas empresas. **Revista da Micro e Pequena Empresa**, v. 19, n. 2, p. 135-164, 2025.

MARIN, Regina Paiva Melo; SOUZA, Jackson Gomes Soares; MARIN, Luciano Heitor Gallegos. Ensinando conceitos básicos de criptografia no ensino médio profissional. **Revista on line de Política e Gestão Educacional**, v. 25, n. 2, p. 1282-1296, 2021. DOI: 10.22633/rpge.v25i2.14469.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **FIPS 180-4: Secure Hash Standard (SHS)**. Gaithersburg: NIST, 2015. Disponível em: https://csrc.nist.gov/pubs/fips/180-4/upd1/final.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.** Gaithersburg: NIST, 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **FIPS 204: Module-Lattice-Based Digital Signature Standard.** Gaithersburg: NIST, 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **FIPS 205: Stateless Hash-Based Digital Signature Standard.** Gaithersburg: NIST, 2024.

OWASP FOUNDATION. **Cryptographic Storage Cheat Sheet.** OWASP Cheat Sheet Series, 2023a.

OWASP FOUNDATION. **Password Storage Cheat Sheet.** OWASP Cheat Sheet Series, 2023b.

PEDRINI, Júlio César Ferreira; CARVALHO, Matheus Almeida de. Diretrizes para aplicação da LGPD em sistemas de software de pequeno porte. **Revista da Micro e Pequena Empresa**, v. 19, n. 1, p. 1-20, 2025. DOI: 10.6034/rmpe.v19i1.2171.

SILVA, Débora Juliane Guerra Marques da; GUARDA, Graziela Ferreira. CriptoData: ensino de criptografia via computação desplugada. In: WORKSHOPS DO CONGRESSO BRASILEIRO DE INFORMÁTICA NA EDUCAÇÃO, 8., 2019, Brasília. **Anais do VIII Congresso Brasileiro de Informática na Educação**, p. 248-257. DOI: 10.5753/cbie.wcbie.2019.248.

SANTOS, Eduardo Emilio dos; CAMPANO JUNIOR, Maurilio Martins; SILVA, Felippe Fernandes da; AYLON, Linnyer Beatrys Ruiz. Cyber Defender: desenvolvimento e avaliação de um jogo educativo para ensino de segurança cibernética. In: SIMPÓSIO BRASILEIRO DE CIBERSEGURANÇA (SBSeg), 2025. **Anais do SBSeg 2025**. DOI: 10.5753/sbseg.2025.10588.