SEGURANÇA DA INFORMAÇÃO EM DOCUMENTOS DIGITAIS: IMPLEMENTAÇÃO DO ALGORITMO AES NA PROTEÇÃO DE ARQUIVOS WORD

João Gabriel Faria Alves, Murilo de Faria da Rosa, Nicolle Fernandes Bicudo, Wagner dos Santos Clementino de Jesus.

Fundação Valeparaibana de Ensino, Colégio Técnico "Antônio Teixeira Fernandes", Curso Técnico em Informática, Rua Paraibuna, 75, Jardim São Dimas, 12245 - 020- São José dos Campos-SP, Brasil, joao.gabrielfa1@gmail.com, murilofariarosa@gmail.com , nicollebicudo@gmail.com , wagner@univap.br.

Resumo

O objetivo deste projeto foi desenvolver uma aplicação desktop, com interface gráfica, para criptografar e descriptografar documentos Word utilizando o algoritmo AES, tornando a proteção de dados acessível a usuários leigos. A aplicação foi desenvolvida em C#, com gerenciamento de usuários, projetos e operações em banco de dados MySQL. Os resultados demonstraram que a solução executa as operações de forma simples e intuitiva. Conclui-se que a combinação de C#, AES e MySQL resulta em uma ferramenta prática e segura para a proteção de arquivos Word.

Área do Conhecimento: Técnico em informática.

Introdução

A crescente digitalização tornou os documentos digitais centrais nas atividades cotidianas, substituindo papéis em razão da agilidade na transmissão de dados (Gandini et al., 2001). Essa modernização exige mecanismos para garantir autenticidade, integridade e confidencialidade (Kim; Solomon, 2014), exigência também presente na Lei Geral de Proteção de Dados Pessoais e na legislação europeia (Masseno, 2020).

Para proteger dados sensíveis, a criptografia transforma informações em formatos ilegíveis para terceiros (Oliveira, 2012). Na criptografia simétrica, que utiliza uma única chave, o Advanced Encryption Standard (AES) é o padrão internacional de referência, destacado por sua eficiência e robustez (Vaz et al., 2023).

O objetivo geral deste trabalho é desenvolver uma aplicação desktop com interface gráfica para criptografia e descriptografia de documentos Word via AES, tornando a proteção acessível a usuários sem conhecimento técnico em segurança da informação.

Metodologia

O desenvolvimento utilizou a linguagem C# na plataforma .NET por ser orientada a objetos e do tipo segura (type-safe) (Dimes, 2016). Como núcleo criptográfico, adotou-se o algoritmo Advanced Encryption Standard (AES), padronizado pelo NIST em 2001 (Terada, 2008). O AES utiliza chave simétrica de 128 bits (16 bytes) para o plaintext, mapeados em matrizes 4x4 que passam por 10, 12 ou 14 rodadas e estágios como Substitute Bytes, Shift Rows, Mix Columns e Add Round Key (Vaz et al., 2023). O AES mantém-se significativamente mais rápido que concorrentes como o 3DES, unindo segurança e desempenho (Pizzuti et al., 2017).

Para o gerenciamento de dados, utilizou-se o SGBD MySQL. A estrutura relacional possui duas tabelas: a de usuários (autenticação, identificação e senha criptografada via senha_hash, conforme boas práticas de segurança em banco de dados) (Silveira, 2022) e a de histórico (registro do arquivo, tipo de execução, data/hora, usuário e caminho gerado), vinculadas por chave estrangeira (1:N).

O fluxo do sistema inicia-se com o login ou cadastro do usuário. Em seguida, é selecionada a operação de criptografia ou descriptografia e indicado o arquivo a ser processado. Ao final, o sistema gera o arquivo correspondente e registra a operação no banco de dados. Esse fluxo é apresentado no diagrama funcional da Figura 1.

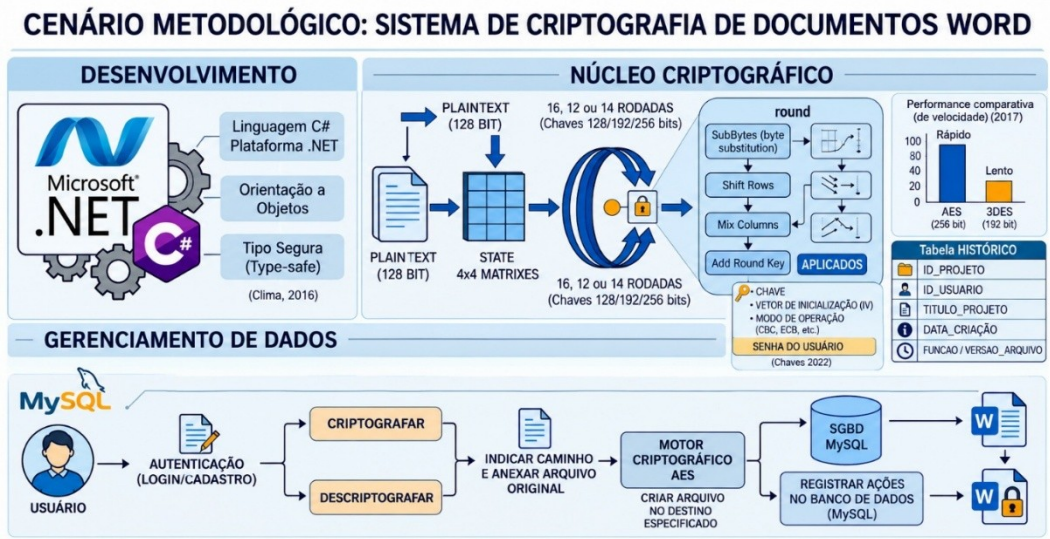


Figura 1: Diagrama de funcionamento do sistema. **Fonte:** Autores, 2026.

Resultados

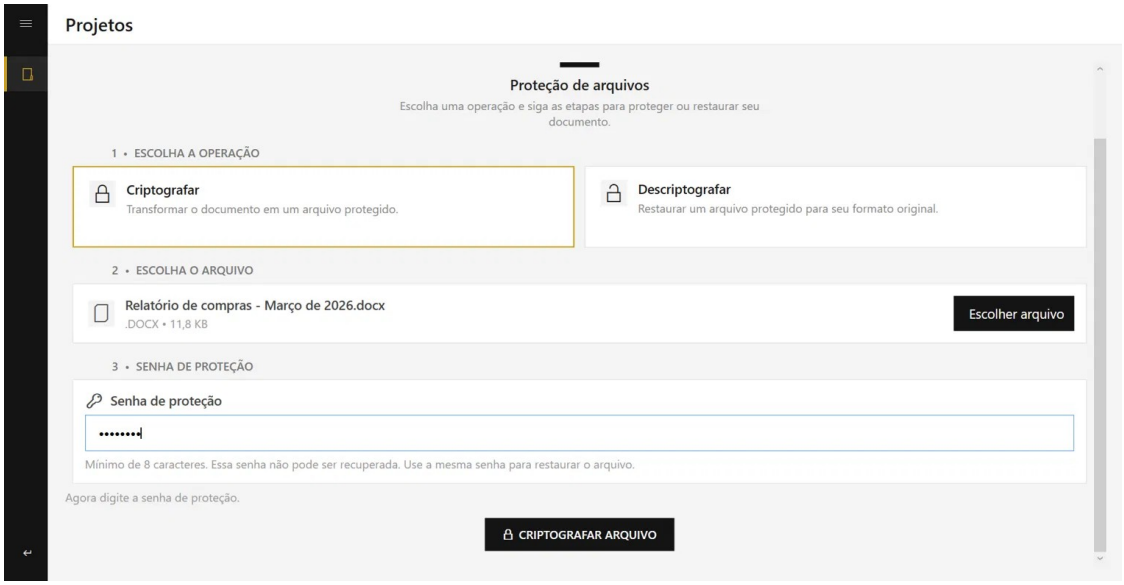
A aplicação permitiu que usuários autenticados realizassem a proteção de documentos do Microsoft Word. A Figura 2 apresenta a tela de detalhes de um projeto com seus dados e arquivos protegidos. A Figura 3 mostra a tela principal do sistema, na qual o usuário seleciona o arquivo e a operação por meio da interface gráfica.

Figura 2: Tela de detalhes do projeto.



Fonte: Autores, 2026.

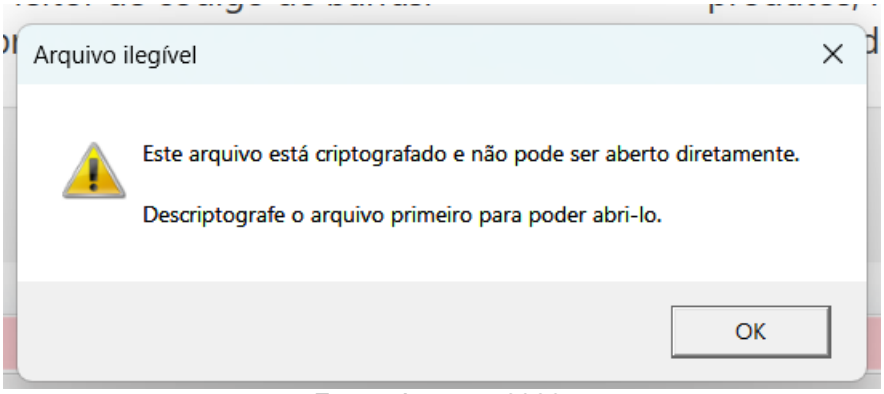
Figura 3: Tela principal do sistema.



Fonte: Autores, 2026.

Ao tentar abrir um arquivo criptografado diretamente sem o processo de descriptografia, o sistema alerta o usuário sobre a inelegibilidade do conteúdo, como mostra a Figura 4.

Figura 4: Abertura de arquivo rejeitada.



Fonte: Autores, 2026.

Discussão

Os resultados indicam que o objetivo do trabalho foi alcançado. A interface gráfica simplifica a proteção de dados para usuários sem conhecimento técnico, enquanto o algoritmo AES garante elevado nível de segurança e o histórico no MySQL provê rastreabilidade e auditoria. Dessa forma, a solução reduz efetivamente a vulnerabilidade de documentos digitais não protegidos. Trabalhos semelhantes de proteção de documentos Word, como o de Mohamed et al. (2015), que combinam criptografia e esteganografia para ocultar conteúdo sensível, reforçam a relevância do tema e apontam caminhos para melhorias futuras.

Conclusão

O projeto cumpriu os objetivos ao disponibilizar uma ferramenta prática e acessível para a criptografia de arquivos do Microsoft Word. A integração entre C#, AES e MySQL mostrou-se eficaz, mitigando riscos de vazamento de documentos digitais sem exigir conhecimentos técnicos avançados dos usuários.

Referências

DA SILVEIRA, Kamilla Dória. Segurança em Banco de Dados para Adequação a LGPD. In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 22., 2022, Santa Maria. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 278-287. DOI: https://doi.org/10.5753/sbseg.2022.223953.

DIMES, Troy. Programação em C# para iniciantes. Tradução de Roger Senna Rosa. [S. l.]: Babelcube, 2016. E-book.

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. A segurança dos documentos digitais. Boletim Jurídico, Uberaba/MG, ano 1, n. 1, 1 ago. 2001. Disponível em: https://www.boletimjuridico.com.br/artigos/direito-e-internet/36/a-seguranca-documentos-digitais. Acesso em: 4 mar. 2026.

KIM, David; SOLOMON, Michael G. Fundamentos de segurança de sistemas de informação. Rio de Janeiro: LTC, 2014.

MASSENO, Manuel David. A segurança dos dados na LGPD, brasileira: uma perspetiva europeia, desde Portugal. Revista do Direito, Santa Cruz do Sul, n. 60, p. 80-103, jan./abr. 2020. DOI: https://doi.org/10.17058/rdunisc.v3i50.14819.

MOHAMED, Mohamed Ahmed; ALTRAFI, Obay G.; ISMAIL, Mohamed O.; ELOBIED, Mawada O. A novel method to protect content of Microsoft Word document using cryptography and steganography. **International Journal of Computer Theory and Engineering**, v. 7, n. 4, p. 292-296, ago. 2015. Disponível em: https://www.ijcte.org/vol7/973-S005.pdf. Acesso em: 24 mar. 2026.

OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. Segurança Digital, [S. l.], v. 31, p. 11-15, 2012.

PIZZUTI, Daniela; SPOLON, Roberta; LOBATO, Renata S.; MANECERO JR., Aleardo. Desempenho dos Algoritmos 3DES e AES Usando Cuda. In: ESCOLA REGIONAL DE ALTO DESEMPENHO DE SÃO PAULO (ERAD-SP), 2017. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2017. p. 25-28. Disponível em: https://sol.sbc.org.br/index.php/eradsp/article/download/4351/4277. Acesso em: 24 ago. 2026.

TERADA, Routo. Segurança de dados: criptografia em redes de computador. 2. ed. rev. e ampl. São Paulo: Blucher, 2008.

VAZ, Yuri Silva; MATTOS, Júlio C. B.; SOARES, Rafael Iankowski. AES Otimizado para Uso em Aplicações IoT. In: Anais Estendidos do Simpósio Brasileiro de Engenharia de Sistemas Computacionais (SBESC), 2023. Porto Alegre: Sociedade Brasileira de Computação, 2023. Disponível em: https://sol.sbc.org.br/index.php/sbesc_estendido/article/download/25853/25681. Acesso em: 7 abr. 2026.