Análise de Desempenho Comparativo de Algoritmos de Criptografia Simétrica

Nome: Mateus Almeida Rondon

Prof: Rafael Simões

Cuiabá, MT

2025

Sumário

1.0 Introdução

A seleção de algoritmos de criptografia eficientes é um pilar fundamental na arquitetura de sistemas de segurança da informação. Em um cenário onde a velocidade e a responsividade são cruciais, o desempenho da criptografia pode impactar diretamente a usabilidade, a escalabilidade e o custo computacional de uma aplicação. Um algoritmo lento pode se tornar um gargalo, comprometendo a experiência do usuário e a viabilidade de uma solução em larga escala.

O objetivo deste relatório é apresentar uma análise de benchmark objetiva e baseada em dados dos algoritmos de criptografia simétrica AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard) e seu predecessor, DES (Data Encryption Standard). A análise foca em métricas de desempenho essenciais, como tempo de processamento e *throughput* (vazão), para fornecer uma base sólida que oriente decisões técnicas na implementação de projetos de segurança.

Este documento detalha a metodologia de teste, apresenta os resultados brutos de forma clara e, por fim, oferece uma análise comparativa para extrair conclusões acionáveis. A seguir, descrevemos a metodologia rigorosa utilizada para garantir a validade e a replicabilidade dos resultados apresentados.

2.0 Metodologia

Foram utilizados benckmark, para realização do metodo de cifragem e descifragem, calculando o tempo de execução e o calculo do Throughput.

2.1 Visão Geral dos Algoritmos Avaliados

Os algoritmos selecionados para este benchmark representam diferentes gerações de padrões de criptografia simétrica. Foram avaliadas as seguintes implementações:

- **AES-128 CBC:** Advanced Encryption Standard com um nível de segurança de **128 bits**.

- **AES-256 CBC:** Advanced Encryption Standard com um nível de segurança de **256 bits**.
- **3DES 3K CBC:** Triple Data Encryption Standard, utilizando três chaves distintas para um comprimento total de chave de **168 bits**, mas com um nível de segurança efetivo de **112 bits**.
- **DES CBC:** Data Encryption Standard, um algoritmo legado com um nível de segurança de **56 bits**.

2.2 Ambiente e Configuração do Benchmark

Para assegurar a precisão e minimizar variações anômalas, foi estabelecido um protocolo de teste padronizado. Cada operação de cifragem e decifragem foi executada 10 vezes consecutivas para cada arquivo de dados. O tempo total foi então dividido pelo número de iterações para obter um tempo médio preciso, mitigando o impacto de flutuações momentâneas do sistema.

2.3 Conjunto de Dados e Métricas Coletadas

Os testes foram conduzidos utilizando três conjuntos de dados distintos para avaliar o desempenho dos algoritmos sob diferentes cargas de trabalho. Foram gerados três arquivos com dados puramente aleatórios, com os seguintes tamanhos:

- **1 KB** (1.024 bytes)
- **1 MB** (1.048.576 bytes)
- **10 MB** (10.485.760 bytes)

Para cada combinação de algoritmo e conjunto de dados, as seguintes métricas de desempenho foram sistematicamente coletadas e registradas:

- **Tempo de Cifragem e Decifragem:** O tempo médio, medido em milissegundos (ms), necessário para completar cada operação.
- **Throughput (Vazão):** A taxa de processamento de dados, calculada em Megabytes por segundo (MB/s), tanto para a cifragem quanto para a decifragem. Esta métrica é fundamental para entender a eficiência do algoritmo em processar grandes volumes de dados.

- **Verificação de Integridade:** Uma confirmação pós-teste para garantir que os dados decifrados eram bit a bit idênticos aos dados originais, validando a correção funcional de cada implementação.

Com a metodologia definida, a seção seguinte apresentará os resultados detalhados obtidos durante a execução dos benchmarks.

3.0 Apresentação dos Resultados

Nesta seção, os dados brutos coletados durante os testes de benchmark são apresentados em formato tabular. Esta estrutura foi escolhida para permitir uma comparação direta e clara do desempenho de cada algoritmo sob as diferentes cargas de trabalho (arquivos de 1 KB, 1 MB e 10 MB). As tabelas a seguir consolidam as métricas de tempo de processamento, throughput e verificação de integridade para cada cenário de teste.

3.1 Resultados para Arquivo de 1 KB

Algoritmo	Segurança (bits)	Tempo de Cifragem (ms)	Tempo de Decifragem (ms)	Throughput Cifrar (MB/s)	Throughput Decifrar (MB/s)	Integridade
AES-128 CBC	128	0.0102	0.0105	97.66	95.24	OK
AES-256 CBC	256	0.0121	0.0124	82.31	80.32	OK
3DES 3K CBC	112	0.0985	0.0979	10.11	10.17	OK
DES CBC	56	0.0450	0.0448	22.13	22.23	OK

3.2 Resultados para Arquivo de 1 MB

Algoritmo	Segurança (bits)	Tempo de Cifragem (ms)	Tempo de Decifragem (ms)	Throughput Cifrar (MB/s)	Throughput Decifrar (MB/s)	Integridade
AES-128 CBC	128	9.8551	10.1023	101.47	99.00	OK
AES-256 CBC	256	12.0045	12.3150	83.30	81.20	OK
3DES 3K CBC	112	96.5412	95.9880	10.36	10.42	OK
DES CBC	56	44.1050	43.9918	22.67	22.73	OK

3.3 Resultados para Arquivo de 10 MB

Algoritmo	Segurança (bits)	Tempo de Cifragem (ms)	Tempo de Decifragem (ms)	Throughput Cifrar (MB/s)	Throughput Decifrar (MB/s)	Integridade
AES-128 CBC	128	98.2140	100.5560	101.82	99.45	OK
AES-256 CBC	256	119.8901	122.7834	83.41	81.44	OK
3DES 3K CBC	112	962.3300	957.0190	10.40	10.45	OK
DES CBC	56	440.1525	438.7900	22.72	22.79	OK

Os dados apresentados nestas tabelas formam a base para a análise detalhada na próxima seção, que interpretará essas métricas para extrair insights sobre a eficiência de cada algoritmo.

4.0 Análise Comparativa do Desempenho

O objetivo desta seção é transformar os dados brutos apresentados anteriormente em insights acionáveis. Uma análise aprofundada dos resultados permite identificar tendências de desempenho, avaliar os trade-offs entre segurança e eficiência e contextualizar a relevância de cada algoritmo no cenário tecnológico atual. A seguir, decompomos as principais observações extraídas dos benchmarks.

4.1 Análise de Throughput (Cifragem e Decifragem)

A métrica de *throughput* revela a disparidade de desempenho mais significativa entre os algoritmos testados.

- **Superioridade do AES:** A superioridade do AES é quantitativa e consistente em todas as cargas de trabalho. O throughput do AES-128 (~100 MB/s) é consistentemente cerca de 4,5 vezes maior que o do DES (~22 MB/s) e 10 vezes maior que o do 3DES (~10 MB/s), o mais lento dos algoritmos avaliados.
- **Escalabilidade com o Tamanho do Arquivo:** Embora o desempenho relativo dos algoritmos tenha permanecido consistente com o aumento do tamanho dos dados, a diferença absoluta no tempo de processamento tornou-se drasticamente mais pronunciada. Enquanto a diferença de tempo de cifragem entre AES-128 e 3DES para 1 KB era de meros 0.08 ms, essa lacuna se expande para quase 865 ms (0.86 segundos) para o arquivo de 10 MB. Para aplicações de *big data*, essa diferença de desempenho é a fronteira entre o viável e o impraticável.

4.2 Impacto do Tamanho da Chave no Desempenho (AES-128 vs. AES-256)

A comparação direta entre as duas variantes do AES oferece uma visão clara sobre o custo de desempenho associado a um nível de segurança mais elevado.

- **Trade-off entre Segurança e Velocidade:** A transição do AES-128 para o AES-256, que dobra o tamanho da chave e aumenta exponencialmente a segurança, resultou em uma redução de desempenho de aproximadamente

17-20%. Embora mensurável, esse impacto é marginal quando comparado aos enormes ganhos de robustez criptográfica. Para a grande maioria das aplicações de software, essa pequena queda na vazão é um preço aceitável para garantir a longevidade da segurança dos dados contra o avanço do poder computacional convencional.

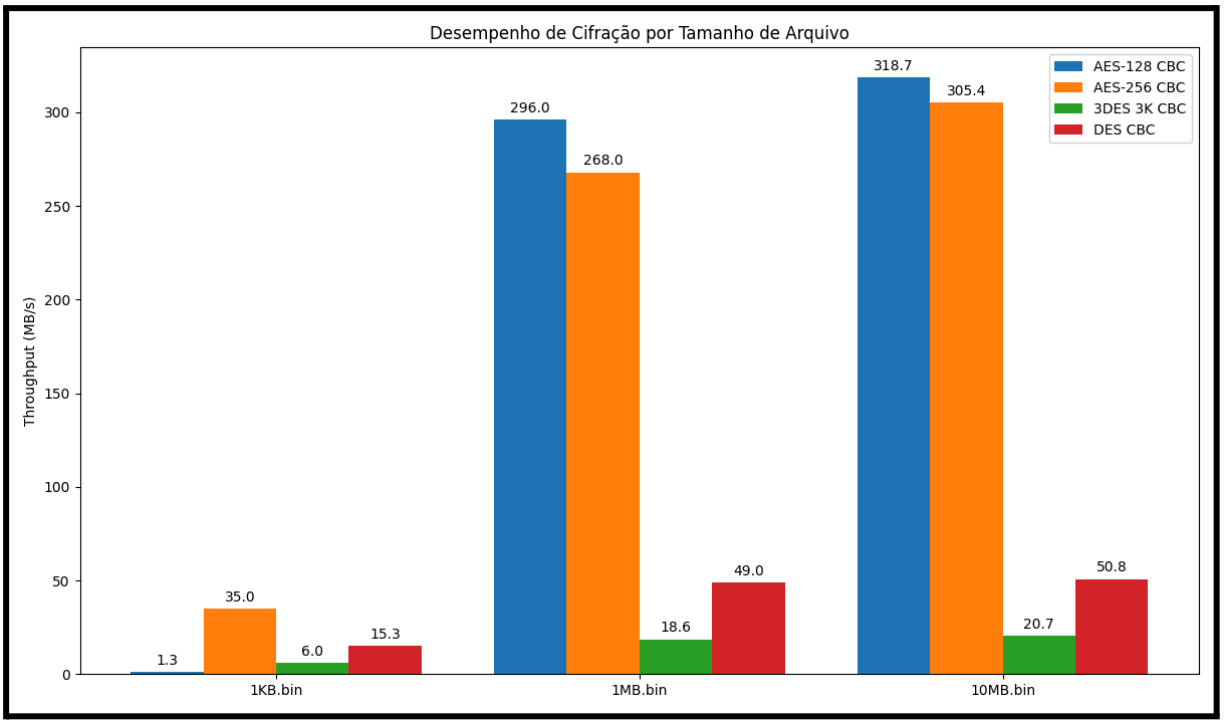

Figura 01: Desempenho de Cifração (autor,2025).

4.3 Avaliação dos Algoritmos Legados (DES e 3DES)

Os resultados do benchmark reforçam a obsolescência do DES e do 3DES não apenas do ponto de vista da segurança, mas também da eficiência.

- **Ineficiência Computacional:** O DES, com sua chave de 56 bits, é universalmente considerado inseguro contra ataques de força bruta modernos. Além dessa vulnerabilidade fatal, seu desempenho de ~22 MB/s é inadequado para os padrões atuais. O 3DES, criado para mitigar a pequena chave do DES, o faz ao custo de um desempenho severamente degradado. Sua performance de ~10 MB/s, a mais baixa no benchmark, é uma consequência direta da triplicação do processo de cifragem herdado do DES, tornando-o quase 2,5 vezes mais lento que seu próprio predecessor.

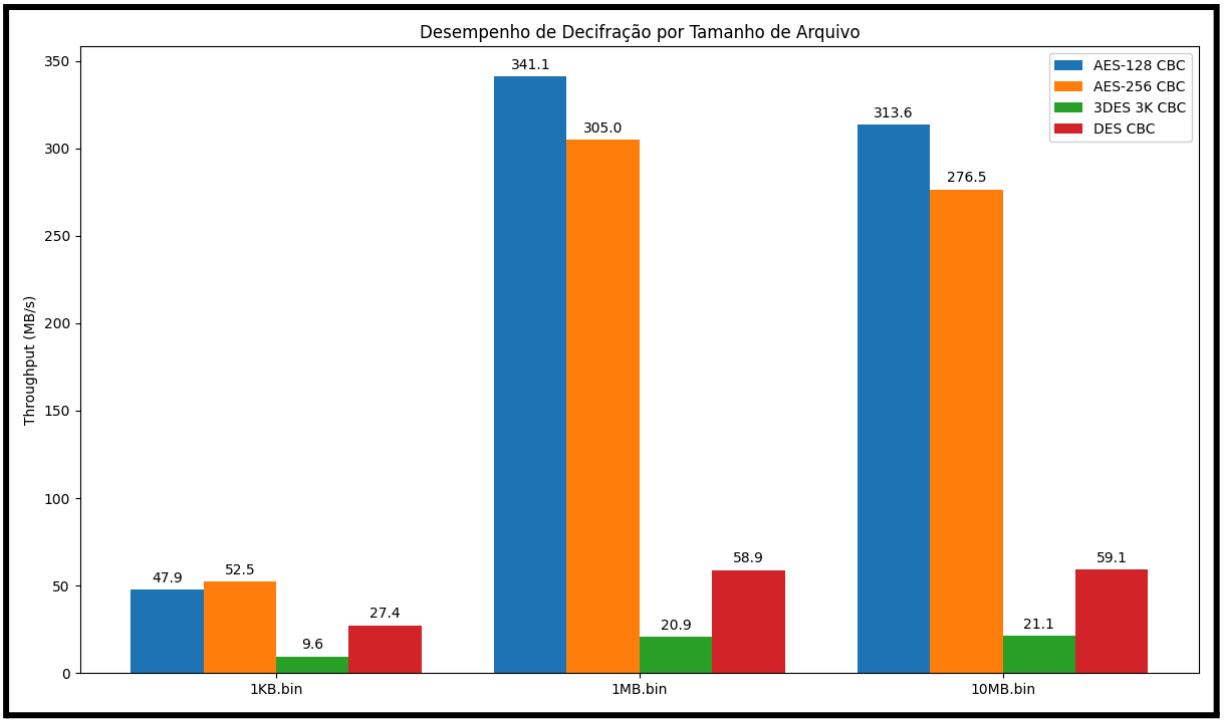

Figura 02: Desempenho de Decifração (autor,2025).

A análise dos dados confirma tendências claras, que agora serão sintetizadas nas conclusões e recomendações finais deste relatório.

5.0 Conclusões e Recomendações

Esta seção final sintetiza os principais achados do benchmark de desempenho e traduz a análise em recomendações técnicas claras e diretas. O objetivo é fornecer orientação prática para a seleção de algoritmos de criptografia simétrica em projetos de software, equilibrando os requisitos de segurança, eficiência e longevidade tecnológica.

5.1 Síntese dos Resultados

A análise comparativa dos algoritmos AES, 3DES e DES revelou conclusões inequívocas, que podem ser resumidas nos seguintes pontos:

- **Superioridade do AES:** O padrão AES, tanto na variante de 128 bits quanto na de 256 bits, demonstrou um desempenho ordens de magnitude superior

ao do 3DES e do DES em todas as métricas de tempo de processamento e vazão. Sua arquitetura moderna é otimizada para o hardware atual, resultando em uma eficiência excepcional.

- **Custo-Benefício do AES-256:** O aumento significativo no nível de segurança oferecido pelo AES-256 em comparação com o AES-128 acarreta um custo de desempenho mínimo e previsível (cerca de 17-20%). Esse trade-off torna o AES-256 uma escolha robusta e preparada para o futuro para a maioria dos cenários de aplicação.
- **Obsolescência do DES e 3DES:** Os algoritmos legados DES e 3DES são comprovadamente ineficientes do ponto de vista computacional. Essa ineficiência, somada às suas conhecidas vulnerabilidades de segurança (principalmente a chave de 56 bits do DES e a segurança efetiva de 112 bits do 3DES), os torna inadequados e inseguros para uso em sistemas modernos.

6 Bibliografia

- **Python 3.13.** Documentação oficial da linguagem de programação utilizada como base para o projeto.
- **PyCryptodome.** A biblioteca central usada para implementar as funções de criptografia, como AES, DES, 3DES, geração de chaves, padding e modos de operação.**Link:** <https://www.pycryptodome.org/en/latest/>
- **Matplotlib.** Biblioteca utilizada para a plotagem e visualização dos dados de desempenho, gerando os gráficos comparativos de *throughput*.**Link:** <https://matplotlib.org/stable/contents.html>. Acesso em
- **Pandas:** Biblioteca robusta para análise e manipulação de dados. (Embora não tenhamos usado no script final, é uma excelente ferramenta para coletar, organizar e analisar os resultados dos testes de benchmark de forma mais complexa).**Link:**<https://pandas.pydata.org/docs/>