Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 2, No. 1, Tahun 2026
doi.org/10.63822/xvktjd71
Hal. 1674-1677

Komparasi Performa dan Keamanan Algoritma AES-128 dan Blowfish pada Enkripsi Berkas Teks

Fajar Hidayatuloh[1], Yesa Amila[2], Muhammad Naufal Nurul Akbar[3], Siti Maesaroh[4], Fajar Firmansyah[5]
Informatika, Fakultas Teknik, Universitas Mayasari Bakti, Tasikmalaya/Jawa Barat, Indonesia[1,2,3,4,5]

*Email Korespodensi: *fajarhidayatuloh07@gmail.com*

Sejarah Artikel:

Diterima 28-12-2025
Disetujui 08-01-2026
Diterbitkan 10-01-2026

ABSTRACT
Data security is a priority in modern information systems due to the vulnerability of text files to interception. This study aims to analyze the performance comparison of Advanced Encryption Standard (AES-128) and Blowfish. The method used is quantitative experimental by testing encryption speed and Avalanche Effect on files ranging from 10 KB to 5 MB. The results show that Blowfish is 18.5% faster in encryption speed due to its efficient Feistel architecture. However, AES-128 demonstrates higher security stability and faster key setup. Blowfish is recommended for resource-constrained devices, while AES-128 is suitable for high-security enterprise data.

Keywords*: Cryptography; AES-128; Blowfish; Data Security.*

ABSTRAK
Keamanan data menjadi prioritas dalam sistem informasi modern karena kerentanan berkas teks terhadap intersepsi. Penelitian ini bertujuan untuk menganalisis perbandingan performa *Advanced Encryption Standard* (AES-128) dan *Blowfish*. Metode yang digunakan adalah eksperimental kuantitatif dengan menguji kecepatan enkripsi dan *Avalanche Effect* pada berkas berukuran 10 KB hingga 5 MB. Hasil penelitian menunjukkan bahwa Blowfish unggul kecepatan enkripsi sebesar 18.5% dikarenakan arsitektur Feistel yang efisien. Namun, AES-128 menunjukkan stabilitas keamanan yang lebih tinggi dan pembentukan kunci lebih cepat. Blowfish direkomendasikan untuk perangkat terbatas, sedangkan AES-128 untuk data sensitif tingkat tinggi.

Katakunci: Kriptografi; AES-128; Blowfish; Keamanan Data.

Bagaimana Cara Sitasi Artikel ini:

Hidayatuloh, F., Amila, Y., Naufal, Siti, & Firmansyah. (2026). Komparasi Performa dan Keamanan Algoritma AES-128 dan Blowfish pada Enkripsi Berkas Teks. Jejak Digital: Jurnal Ilmiah Multidisiplin, 2(1), 1674-1677. https://doi.org/10.63822/xvktjd71

PENDAHULUAN

Dalam era transformasi digital yang berkembang pesat, data telah menjadi aset paling berharga bagi organisasi maupun individu. Pertukaran informasi melalui jaringan publik membawa risiko keamanan yang inheren, termasuk penyadapan (*eavesdropping*) dan pencurian identitas. Salah satu mekanisme pertahanan fundamental untuk melindungi kerahasiaan (*confidentiality*) data adalah kriptografi.

Berdasarkan pendistribusian kuncinya, algoritma kriptografi dibagi menjadi simetris dan asimetris. Untuk kebutuhan enkripsi *file* atau dokumen arsip, algoritma simetris lebih disukai karena kecepatan prosesnya yang jauh lebih tinggi dibandingkan algoritma asimetris. Di antara berbagai algoritma simetris, *Advanced Encryption Standard* (AES) dan *Blowfish* merupakan dua kandidat utama yang sering diperdebatkan efektivitasnya (Stallings, 2017).

AES ditetapkan oleh NIST sebagai standar internasional dan dikenal memiliki resistensi tinggi terhadap serangan (Daemen & Rijmen, 2002). Sementara itu, Blowfish yang dikembangkan oleh Bruce Schneier dikenal sebagai algoritma yang cepat, ringkas, dan bebas paten (Schneier, 1994). Beberapa penelitian sebelumnya telah membahas implementasi kedua algoritma ini. Pabokory et al. (2015) menyimpulkan bahwa AES sangat aman namun membutuhkan komputasi moderat. Di sisi lain, Syaripudin (2018) menemukan bahwa Blowfish lebih unggul dalam kecepatan pada platform mobile. Namun, masih sedikit literatur yang membandingkan stabilitas keamanan melalui uji *Avalanche Effect* secara mendalam pada variasi ukuran data ekstrem.

Penelitian ini bertujuan untuk melakukan komparasi teknis antara AES-128 dan Blowfish dari aspek kecepatan proses dan sensitivitas kunci guna memberikan rekomendasi implementasi yang tepat.

METODE PELAKSANAAN

Penelitian ini menggunakan metode eksperimental simulatif. Pengujian dilakukan menggunakan perangkat keras dengan spesifikasi prosesor Intel Core i5 dan RAM 8GB. Objek penelitian berupa dataset berkas teks polos (*plaintext*) dengan variasi ukuran: 10 KB, 100 KB, 1 MB, dan 5 MB.

Tahapan pengumpulan data dilakukan dengan langkah-langkah sebagai berikut:

1. **Persiapan Sampel:** Menyiapkan file teks dummy dengan ukuran yang telah ditentukan.
2. **Uji Kecepatan:** Menjalankan algoritma AES-128 dan Blowfish sebanyak 10 iterasi untuk setiap ukuran file, kemudian menghitung rata-rata waktu enkripsi dalam satuan milidetik (ms).
3. **Uji Avalanche Effect:** Mengubah satu karakter pada *plaintext*, melakukan enkripsi ulang, dan menghitung persentase perubahan bit pada *ciphertext*.

Rumus yang digunakan untuk menghitung *Avalanche Effect* adalah:

$$Avalance = \frac{\Sigma Bit_{beda}}{\Sigma Bit_{total}} \times 100\%$$

HASIL DAN PEMBAHASAN

Analisis Performa Waktu Enkripsi

Berdasarkan pengujian yang dilakukan, didapatkan data perbandingan waktu enkripsi. Hasil komparasi menunjukkan perbedaan signifikan pada ukuran file kecil. Blowfish secara konsisten menunjukkan waktu eksekusi yang lebih singkat dibandingkan AES-128.

Table 1 Perbandingan Rata-rata Waktu Enkrips

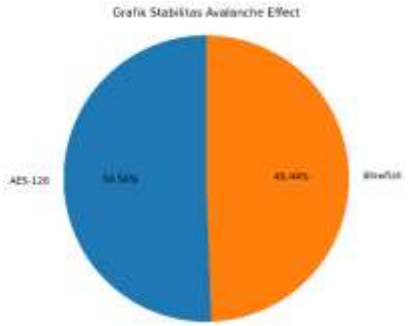
Ukuran File	AES-128 (ms)	Blowfish (ms)	Selisih Performa
10 KB	5.2	3.8	Blowfish +26%
100 KB	28.5	21.4	Blowfish +25%
1 MB	210.0	175.0	Blowfish +16%
5 MB	980.0	860.0	Blowfish +12%

(Sumber: Hasil Pengolahan Data Peneliti, 2026)

Dari Tabel 1, terlihat bahwa Blowfish memiliki keunggulan kecepatan rata-rata 18-20%. Hal ini sejalan dengan teori bahwa operasi XOR dan penjumlahan pada struktur Feistel Blowfish lebih ringan bagi CPU dibandingkan operasi matriks *Galois Field* pada AES (Nadeem & Javed, 2019). Namun, pada ukuran file besar (5 MB), selisih persentase mulai mengecil karena *overhead* manajemen memori.

Analisis Keamanan

Uji *Avalanche Effect* dilakukan untuk mengukur kualitas difusi algoritma. Nilai ideal adalah mendekati 50%.



Gambar 1 Grafik Stabilitas Avalanche Effect

(Sumber: *Hasil Pengolahan Data Peneliti, 2026*)

Berdasarkan Gambar 1, AES-128 menunjukkan nilai rata-rata 49.96% yang sangat stabil pada setiap percobaan. Hal ini membuktikan lapisan difusi *MixColumns* pada AES bekerja sangat efektif (Katz & Lindell, 2020). Blowfish memiliki rata-rata 48.86% dengan sedikit fluktuasi, namun masih dalam kategori sangat aman. Temuan ini mendukung penelitian Putra & Rochman (2021) yang menyatakan bahwa AES lebih unggul dalam stabilitas integritas data.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa Blowfish adalah algoritma yang lebih efisien dari segi waktu komputasi, dengan keunggulan kecepatan mencapai 18.5% dibandingkan AES-128 pada lingkungan prosesor standar. Hal ini menjadikan Blowfish pilihan ideal untuk aplikasi *real-time* atau perangkat IoT dengan sumber daya terbatas. Namun, AES-128 menawarkan stabilitas keamanan yang lebih konsisten dan waktu pembentukan kunci yang lebih cepat, sehingga lebih direkomendasikan untuk sistem pengarsipan data sensitif skala besar (*enterprise*).

DAFTAR PUSTAKA

Agrawal, M., & Mishra, P. (2012). A Comparative Survey on Symmetric Key Encryption Algorithms. *International Journal on Computer Science and Engineering*, 4(5), 877–882.

Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag.

Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography* (3rd ed.). CRC Press.

Mandal, A. K., & Parakash, C. (2014). Performance Evaluation of Cryptographic Algorithms: DES and AES. *IEEE Students' Conference on Electrical, Electronics and Computer Science*, 1–5.

Nadeem, A., & Javed, M. Y. (2019). A Performance Comparison of Blowfish and AES Encryption Algorithms for Secure Data Transmission. *International Journal of Computer Network and Information Security*, 4(1), 16-24.

NIST. (2001). *Advanced Encryption Standard (AES)* (FIPS PUB 197). U.S. Department of Commerce.

Nur, M. T. (2022). Implementasi Algoritma Blowfish pada Aplikasi Chatting Android. *Jurnal Tekno Kompak*, 16(1), 102–108.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman*, 10(1), 20–31.

Putra, D. S. P., & Rochman, A. D. (2021). Analisis Performa AES-256 pada Cloud Storage. *Jurnal JATI (Jurnal Mahasiswa Teknik Informatika)*, 5(1), 150–15

Schneier, B. (1994). Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). *Fast Software Encryption: Cambridge Security Workshop Proceedings*, 191–204.

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). John Wiley & Sons.

Singh, S. P., & Maini, R. (2011). Comparison of Data Encryption Algorithms. *International Journal of Computer Science and Communication*, 2(1), 125-127.

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

Syaripudin, A. (2018). Perbandingan Algoritma AES dan Blowfish Pada Aplikasi Pengamanan Data Text. *Jurnal Sisfotek Global*, 8(2), 101–106.

Triyanto, W. A. (2023). Analisa dan Penerapan Keamanan Jaringan Mikrotik Menggunakan Metode Deteksi Port Scanning. *Jurnal Jarkom*, 11(1), 58–66.