E-ISSN : 2827-8550
P- ISSN : 1978-5569

ANALISIS KINERJA ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) ENCRYPTION DAN ALGORITMA BLOWFISH PADA PROSES ENKRIPSI DAN DEKRIPSI

Fajar Dwi Insani[1)], Meita Dwi Anggraeni[2)]

[1)] "Bisnis Digital" Universitas Muhammadiyah Kudus
[2)] "Teknik Informatika" STMIK BINA PATRIA Magelang
Email : Insanifajardwi@gmail.com[1)], Meitadww@gmail.com[2)]

Abstract

The rapid development of information technology has encougraged organizations to utilize database technologies in managing information, creating a need for security methods capable of ensuring data confi*dentiality, integrity, and authentication. Cryptography serves as a primary solution for protecting digital files, including through the use of Pretty Good Privacy (PGP), which provides both encryption and digital signature features. This study examines the performance comparison of two widely used modern cryptographic algorithms: Blowfish and the Advanced Encryption Standard (AES). Blowfish is known as a strong and resilient block cipher, while AES is the cryptographic standard recommended by NIST, offering key lengths of 128, 192, and 256 bits. The evaluation is conducted based on data size as a benchmark to determine the optimal encryption processing time for each algorithm. The analysis reveals notable performance differences, which can serve as a reference for developers in selecting the most suitable encryption algorithm for their applications, as well as a resource for further research related to AES and Blowfish encryption algorithms.*

Keywords: ***Cryptography, Blowfish, AES, Encryption, Performance.***

Abstrak

Perkembangan teknologi informasi mendorong organisasi untuk memanfaatkan teknologi basis data dalam pengelolaan informasi, sehingga dibutuhkan metode pengamanan yang mampu menjaga kerahasiaan, integritas, dan otentikasi data. Kriptografi menjadi solusi utama dalam melindungi file digital, termasuk melalui perangkat lunak Pretty Good Privacy (PGP) yang menyediakan fitur enkripsi dan tanda tangan digital. Penelitian ini membahas perbandingan performa dua algoritma kriptografi modern yang banyak digunakan, yaitu Blowfish dan Advanced Encryption Standard (AES). Blowfish dikenal sebagai cipher block yang kuat dan sulit ditembus, sedangkan AES merupakan standar kriptografi yang direkomendasikan NIST dengan panjang kunci 128, 192, dan 256 bit. Pengujian dilakukan berdasarkan ukuran data sebagai pembanding untuk memperoleh waktu proses enkripsi terbaik pada masing-masing algoritma. Hasil analisis menunjukkan adanya perbedaan performa yang dapat menjadi acuan bagi pengembang dalam memilih algoritma yang paling sesuai dengan kebutuhan aplikasi, serta menjadi referensi untuk penelitian lanjutan terkait algoritma enkripsi.

Kata kunci: Kriptografi, Blowfish, AES, Enkripsi, Performa.

1. Pendahuluan

Perkembangan Teknologi informasi telah membawa perubahan besar terhadap cara manusia dan organisasi menjalankan aktivitas serta mengelola data mereka. Perkembangan teknologi juga terjadi di beberapa sektor penting, seperti ekonomi, pendidikan, sosial, hukum, dan lain sebagainya (Susilo E.K, 2021). Sistem-sistem pada dunia informasi dan teknologi masih banyak yang belum menerapkan keamanan digital seperti kriptografi, dengan perkembangan teknologi yang semakin pesat diiringi juga serangan digital yang

E-ISSN : 2827-8550
P- ISSN : 1978-5569

rentan dan masif dan didukung internet dengan penyebarannya meluas digunakan sarana berkomunikasi dan mencari informasi, berkomunikasi yang saling mengirim dan menerima informasi menggunakan proses enkripsi dan deskripsi ((Dedek Indra Gunawan Hts, 2023).

Keamanan penting dalam penyimpanan dan pengiriman informasi atau pesan. Keamanan dapat didefinisikan sebagai proses, prosedur, dan kebijakan yang dipakai untuk menutup akses yang tidak sah. Memecahkan masalah, mengekspos, mengganggu, dan mengganti sumber daya jaringan komputer (Zaenul Arif, 2023). Dalam hal ini perlu diperhatikan bahwa keamanan sistem informasi harus dijaga kerahasiaannya agar informasi siap diterima oleh penerima dan dapat dikirim dengan cara yang dirahasiakan oleh orang lain yang tidak berwenang (Zaenul Arif, 2023). Ini hanya boleh dibaca oleh penerima dan dapat dirahasiakan oleh pengirim (M. I. Afandi, 2021). Ada cabang ilmu yang mempelajari privasi data atau informasi, yaitu kriptografi (Dola Ramalinda, 2024). Secara etimologi kata kriptografi (*Cryptography*) berasal dari bahasa Yunani, yaitu *kryptos* yang artinya yang tersembunyi dan *graphein* yang berarti tulisan (Ariska, 2022). Kriptografi bertugas menjaga keamanan sebuah data menggunakan metode penyisipan data dengan suatu algoritma khusus dengan tujuan data tersebut terlindungi dari pengguna lain. Teknik ini selain mengubah data, dapat juga dipakai untuk melindungi integritas, keaslian serta nirsangkal (Yoga Pratama, 2023). Pada penelitian ini penulis menggunakan dua algoritma untuk penelitian ini yaitu algoritma Blowfish dan Advanced Encryption Standard (AES).

Schneier, sebagai pengembang utama algoritma Blowfish, menjelaskan dalam publikasinya bahwa algoritma ini dirancang sebagai solusi kriptografi yang bebas dari pembatasan paten dan dimaksudkan untuk dapat digunakan secara luas di ranah publik. Di bidang kriptografi modern, Blowfish memperoleh posisi tersendiri karena menawarkan kinerja enkripsi yang cepat, tingkat keamanan yang kuat, serta ketersediaannya yang tidak dibatasi oleh persyaratan lisensi (Nuniek Fahriani, 2021).

AES (Advanced Encryption Standard) merupakan algoritma kriptografi berbasis cipher blok yang bekerja dengan ukuran blok tetap sebesar 128 bit. Standar ini dikembangkan sebagai pengganti DES (Data Encryption Standard) karena menawarkan tingkat keamanan yang lebih tinggi dan lebih tahan terhadap serangan modern. Mekanisme enkripsi maupun dekripsi pada AES dilakukan melalui sejumlah putaran proses yang berurutan, meliputi tahapan substitusi byte, pergeseran baris, pencampuran kolom, serta penerapan operasi XOR dengan kunci enkripsi (Yusril Agita Prayoga Tarigan, 2024).

2. Metode Penelitian

Metode penelitian yang dipergunaakan pada penelitian ini meliputi studi literatur, pengumpulan data uji, dan rancangan serta implementasi objek penelitian, pengujian, dan pengolahan data uji, dan terakhir pengambilan kesimpulan. Berikut adalah alur atau flowchart yang digunakan pada penelitian ini.

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Gambar 1. *Flowchart*

2.1 Studi Literature

2.1.1 Perhitungan Algoritma Blowfish

Algoritma Blowfish merupakan salah satu algoritma kriptografi kunci simetri, di mana proses enkripsi dan dekripsi menggunakan kunci yang sama sehingga menjaga konsistensi dan integritas proses pengamanan data. Blowfish digolongkan sebagai block cipher, yang berarti bahwa selama proses enkripsi maupun dekripsi, algoritma ini akan memecah pesan menjadi blok-blok data berukuran tetap. Pada Blowfish, setiap blok memiliki ukuran 64-bit, sehingga pesan yang panjangnya tidak merupakan kelipatan delapan byte harus melalui proses penambahan bit tambahan (padding) agar seluruh blok memiliki ukuran yang seragam.

Secara konseptual, algoritma Blowfish tersusun atas dua komponen utama, yaitu key expansion dan data encryption. Tahap key expansion berfungsi memperluas kunci utama berukuran 56 byte menjadi serangkaian subkunci dengan total ukuran mencapai sekitar 4168 byte. Subkunci ini dibentuk dalam beberapa array yang nantinya digunakan pada setiap tahap enkripsi. Sementara itu, proses data encryption dilakukan pada struktur Feistel network dengan jumlah pengulangan sebanyak enam belas putaran. Setiap putaran terdiri dari operasi

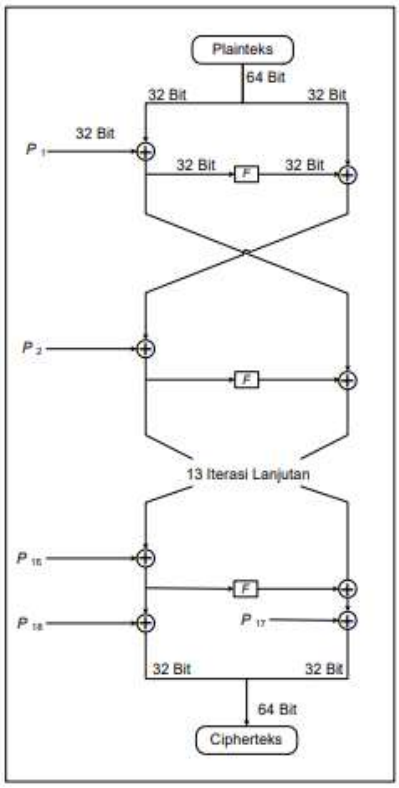
E-ISSN : 2827-8550
P- ISSN : 1978-5569

permutasi yang tidak bergantung pada kunci serta proses substitusi yang tidak bergantung pada data maupun kunci secara langsung. Operasi dasar yang digunakan mencakup penjumlahan modulo serta XOR terhadap word 32-bit, disertai akses terhadap empat indeks array (lookup table) pada setiap iterasi.

Karena Blowfish bergantung pada banyak subkunci untuk menyelesaikan proses enkripsi dan dekripsi, seluruh subkunci tersebut harus dihitung dan dibangkitkan terlebih dahulu sebelum algoritma dapat beroperasi secara efektif. Tahap inisialisasi ini menjadi penting untuk memastikan bahwa proses kriptografi berjalan optimal dan mampu memberikan tingkat keamanan yang memadai terhadap data yang diproses. Kunci yang digunakan termasuk 18 sub kunci 32 bit yang dikelompokkan dalam array **P** (P1, P2, hingga P18). Selain itu, terdapat juga empat S-box 32 bit, masing-masing dengan 256 entri: S1,0, S1,1, hingga S1,255; S2,0, S2,1, hingga S2,255; S3,0, S3,1, hingga S3,255; S4,0, S4,1, hingga S4,255.

Pada jaringan feistel, Blowfish memiliki 16 iterasi, masukannya adalah 64-bit elemen data, X. Untuk melakukan proses enkripsi :

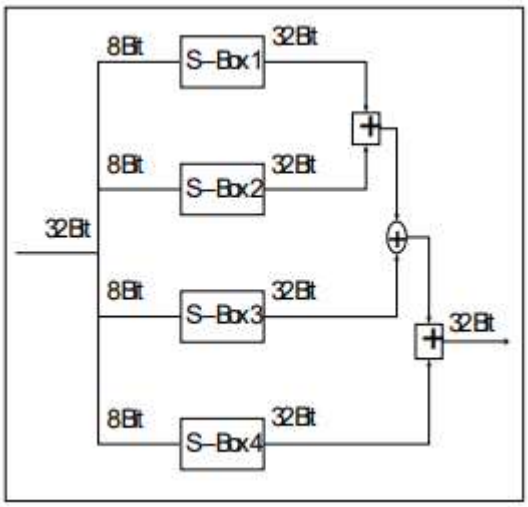
1. Bagi X menjadi dua bagian yang masing-masing terdiri dari 32-bit: XL, XR.
2. For i = 1 to 16: XL = XL XOR Pi XR = F(XL) XOR XR Tukar XL dan XR
3. Setelah iterasi ke-enam belas, tukar XL dan XR lagi untuk melakukan undo pertukaran terakhir.
4. Lalu lakukan XR = XR XOR P17 XL = XL XOR P1
5. Terakhir, gabungkan kembali XL dan XR untuk mendapatkan cipherteks. Untuk lebih jelasnya, gambaran tahapan pada jaringan feistel yang digunakan Blowfish adalah seperti pada Gambar 2



Gambar 2. Struktur Dasar Algoritma Blowfish

E-ISSN : 2827-8550
P- ISSN : 1978-5569

Pada langkah berikutnya, sudah dituliskan mengenai penggunaan fungsi F. Fungsi F adalah :
XL dibagi menjadi empat bagian 8-bit: a, b, c dan d. F (XL) = ((S1,a+S2,b mod 232) XOR S3, c) + S4,d mod 232.
Untuk dapat lebih memahami fungsi F, tahapannya bisa dilihat pada gambar 3



Gambar 3. Diagram Fungsi F pada Algoritma Blowifsh

Algoritma Blowfish ini memiliki keunikan atau pembeda dalam hal proses dekripsi, pembeda atau keunikan tersebut terletak pada proses dekripsi yang dilakukan dengan urutan yang sama persis dengan proses enkripsi, hanya saja pada proses dekripsi P1, P2, hingga P18 digunakan dalam urutan yang terbalik.
Sebelumnya telah dijelaskan mengenai penggunaan subkunci dalam Blowfish. Sekarang, kemudian akan dijelaskan bagaimana cara menghitung atau membangkitkan subkunci :

1. Inisialisasi P-array pertama dan empat S-box, secara berurutan, dengan string yang telah ditentukan. String tersebut terdiri atas digit heksadesimal dari pi, tanpa menggunakan tiga angka pertama.
   Contoh:
   P1 = 0x243f6a88
   P2 = 0x85a308d3
   P3 = 0x13198a2e
   P4 = 0x03707344
2. XOR p1 dengan 32 bit pertama dari kunci, XOR p2 dengan 32 bit kedua dari kunci, dan seterusnya pada semua bit dari kunci (sampai p18). Ulangi siklus tersebut untuk semua bit kunci secara berurutan sampai semua elemen P-array telah di-XOR-kan dengan bit-bit kunci.
3. Kemudian lakukan enkripsi pada string yang semuanya nol (all-zero) menggunakan algoritma Blowfish disertai subkunci yang telah dijelaskan pada langkah (1) dan (2).
4. Ubah p1 dan p2 dengan hasil dari langkah (3).

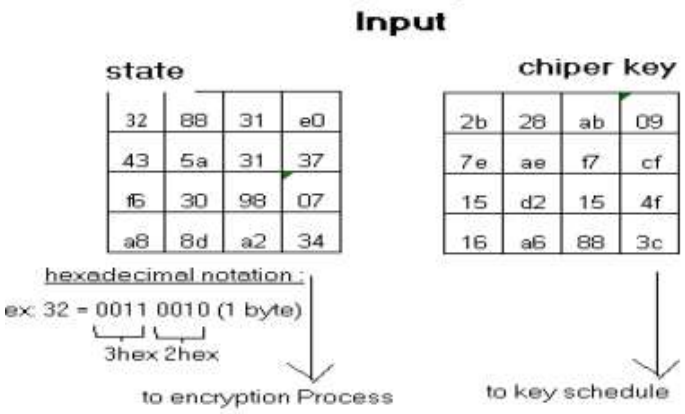
E-ISSN : 2827-8550
P- ISSN : 1978-5569

5. Lakukan enkripsi pada hasil dari tahap (3) menggunakan algoritma Blowfish dengan subkunci yang telah dimodifikasi.
6. Lalu ubah p3 dan p4 dengan hasil dari langkah (5).
7. Lanjutkan tahapan-tahapan di atas, gantikan semua elemen dari P-array dan kemudian empat S-box secara berurutan dengan hasil yang terus berubah dari algoritma Blowfish.

Secara keseluruhan, dibutuhkan 521 iterasi untuk membangkitkan semua subkunci. Aplikasi dapat menyimpan semua subkunci untuk menghindari mengeksekusi proses ini berulang-ulang setiap iterasi.

2.1.2 Perhitungan Algoritma AES

Tahap selanjutnya yang dilakukan pada penelitian ini dimulai dari mempelajari diagram tentang kriptografi, khususnya algoritma AES (Arther Ignasius Suranta, 2022). Sebelum memasuki tahap perancangan aplikasi berbasis algoritma AES, diperlukan terlebih dahulu analisis menyeluruh terkait mekanisme kerja AES, mulai dari proses enkripsi hingga data dapat dikembalikan ke bentuk semula melalui proses dekripsi. Analisis ini bertujuan untuk memastikan bahwa seluruh tahapan yang terlibat dalam algoritma dapat dipahami secara konseptual maupun teknis. Sebagai ilustrasi, berikut ditunjukkan contoh implementasi proses enkripsi pada putaran (round) pertama, di mana blok plaintext dan kunci utama yang direpresentasikan dalam format heksadesimal dikenakan operasi XOR sebagai langkah awal pembentukan state sebelum memasuki transformasi berikutnya dalam struktur enkripsi AES.



Gambar 4. Diagram Input State dan Cipher Key pada Algoritma AES

Pada algoritma AES, baik data masukan maupun data keluaran direpresentasikan dalam bentuk rangkaian bit berukuran 128 bit. Rangkaian bit yang telah diorganisasikan ke dalam satu unit berukuran 128 bit tersebut disebut sebagai blok data atau plaintext, yang selanjutnya diproses melalui mekanisme enkripsi sehingga menghasilkan ciphertext.

AES (Advanced Encryption Standard) mendukung panjang kunci 128, 192, dan 256 bit, sehingga konfigurasi tersebut berbeda dari jumlah putaran pada algoritma Rijndael yang menjadi basisnya. Pada AES dengan kunci 128 bit, digunakan empat kata kunci (masing-masing berukuran 32 bit) sehingga total panjang kunci mencapai 128 bit, dengan ukuran blok plaintext 128 bit dan jumlah putaran proses sebanyak sepuluh kali. Seluruh byte yang terlibat dalam proses AES diperlakukan sebagai elemen pada finite

E-ISSN : 2827-8550
P- ISSN : 1978-5569

field, di mana operasi penjumlahan maupun perkaliannya mengikuti aturan aljabar khusus yang tidak sama dengan operasi bilangan konvensional. Pada tahap SubBytes(), setiap byte dalam state array ditransformasikan melalui S-box yang berfungsi sebagai tabel substitusi non-linear.

2.2 Pengumpulan Data Uji

Data yang dimanfaatkan dalam penelitian ini diambil dari kumpulan kata sandi yang telah ada dan dipublikasikan secara terbuka (open source) melalui repositori daring https://github.com/duyet/bruteforce-database, sehingga dapat diakses oleh siapapun secara gratis dan tidak perlu permohonan izin.

Kumpulan data tersebut terdiri atas 38.650 entri kata sandi, yang masing-masing memiliki variasi panjang serta kombinasi karakter yang beragam. Seluruh data uji tersebut kemudian digunakan sebagai dasar analisis untuk mengevaluasi performa algoritma pada berbagai kondisi kompleksitas kata sandi.

2.3 Perancangan dan Implementasi

Pada penelitian ini akan menguji performa dari algoritma blowfish dan AES dengan dataset password yang telah dikumpulkan, pengujian dari masing-masing algoritma akan diuji masing-masing 3 kali key dengan perubahan parameter key sebanyak 16,24,36 bit yang di generate random. Pengujian akan menggunakan bahasa pemrograman Python 3.9 dengan library pycryptodome.

2.4 Analisa Data Uji

Setiap teknik yang digunakan untuk mengenkripsi memiliki kelebihan dan kekurangan masing-masing. Untuk dapat menerapkan algoritma kriptografi pada sebuah studi kasus, diharuskan memiliki pengetahuan tentang kinerja, kelebihan, dan kekurangan dari algoritma tersebut. Oleh karena itu, algoritma tersebut harus dianalisis secara tepat karena akan sangat mempengaruhi hasil dari penelitian. Pada penelitian ini akan berfokus pada kinerja proses enkripsi dan proses dekripsi pada tiap-tiap algoritma.

2.4.1 Waktu Enkripsi

Waktu yang diperlukan untuk dapat mengubah plaintext menjadi ciphertext bergantung pada ukuran kunci dan blok plainteks. Pada percobaan yang sudah kami lakukan, kami telah mengukur waktu enkripsi dalam milidetik. Waktu enkripsi berpengaruh pada kinerja enkripsi. Waktu enkripsi yang lebih sedikit menunjukkan bahwa algoritma tersebut efektif dan efisien.

2.4.2 Waktu Dekripsi

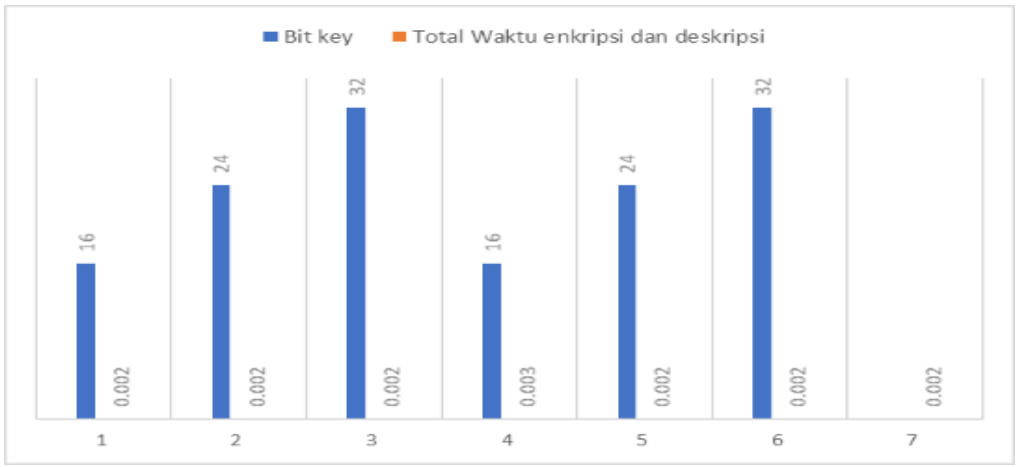
Waktu yang dibutuhkan untuk mengembalikan plaintext dari ciphertext disebut waktu dekripsi. Waktu dekripsi yang diharapkan sebanding dengan waktu enkripsi untuk membuat algoritma responsif dan cepat. Waktu dekripsi berpengaruh pada kinerja sistem. Dalam percobaan, waktu yang digunakan untuk mengukur adalah milidetik.

3. Hasil dan Pembahasan

3.1 *Hasil Penelitian*

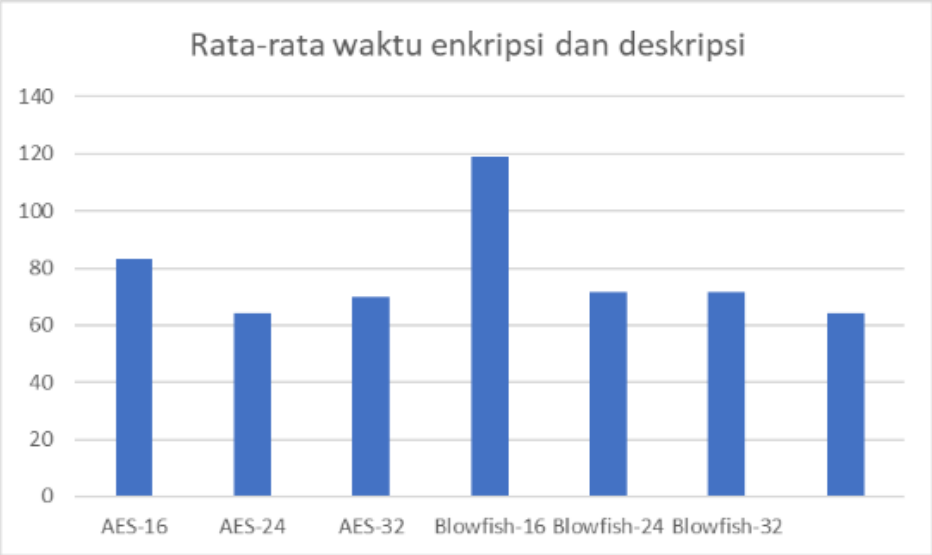
Hasil penelitian ini dibuat dalam bentuk tabel agar lebih mudah untuk dianalisis.

E-ISSN : 2827-8550
P- ISSN : 1978-5569



Gambar 5. Total Waktu

Hasil dari gambar diatas menunjukan bahwa AES (*Advanced Encryption Standard)* dengan parameter key 24 bit lebih cepat dibanding yang lain dalam hal total waktu yang dibutuhkan dan rata-rata 64.3 detik.



Gambar 6. Rata-Rata Waktu

Untuk rata-rata yang di butuhkan untuk enkripsi dan dekripsi hasil terbaik didapatkan oleh AES dengan parameter key 24 bit yang mencapai 0.00016 detik untuk satu kali enkripsi hal ini di karenakan AES (*Advanced Encryption Standard*) menggunakan fungsi putaran yang lebih sederhana dan memiliki struktur yang lebih teratur, yang memudahkan untuk dianalisis dan dioptimalkan dalam segi kecepatan.

4. Kesimpulan

Berdasarkan hasil pengujian yang dilakukan terhadap aspek kecepatan pemrosesan, dapat diinterpretasikan bahwa algoritma kriptografi AES (*Advanced Encryption Standard)* dengan parameter kunci 24-bit menunjukkan performa yang

E-ISSN : 2827-8550
P- ISSN : 1978-5569

lebih unggul dibandingkan Blowfish. Hal ini terlihat dari kemampuan AES dalam menyelesaikan proses enkripsi dengan waktu yang relatif lebih singkat. Keunggulan tersebut dipengaruhi oleh karakteristik AES (*Advanced Encryption Standard)* yang menggunakan ukuran blok tetap sebesar 128 bit, sehingga jumlah putaran (round) yang dibutuhkan untuk mengenkripsi setiap blok data menjadi lebih efisien.

Sebaliknya, algoritma Blowfish memiliki rentang ukuran kunci yang cukup luas, yaitu antara 32 bit hingga 448 bit, sehingga mekanisme pemrosesan datanya cenderung lebih kompleks. Variasi panjang kunci tersebut menyebabkan jumlah operasi yang harus dilakukan pada setiap putaran enkripsi menjadi lebih besar, yang pada akhirnya berdampak pada meningkatnya waktu eksekusi secara keseluruhan.

Dengan mempertimbangkan hasil pengukuran performa tersebut, dapat ditegaskan bahwa AES merupakan pilihan yang lebih tepat untuk kebutuhan enkripsi yang memprioritaskan kecepatan, seperti pada proses pengamanan password. Efisiensi putaran enkripsi yang dimiliki AES (*Advanced Encryption Standard)* memungkinkan algoritma ini memproses data dalam waktu yang sangat singkat, bahkan pada skala detik, sehingga memenuhi tuntutan penggunaan pada sistem yang membutuhkan respons cepat dan stabil.

Daftar Pustaka

Ariska, W. (2022). PENERAPAN KRIPTOGRAFI MENGGUNAKAN ALGORITMA DES (DATA ENCRYPTION STANDARD). *Sintaks Logika (JSilog)*, 1-11.

Arther Ignasius Suranta, D. V. (2022). Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi. *Sistem Komputer dan Teknik Informatika*, 1-10.

Dedek Indra Gunawan Hts, M. R. (2023). Perbandingan Algoritma Kriptografi Simetris dan Asimetris. *UNES Journal of Information System*, 1-6.

Dola Ramalinda, J. A. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*, 1-7.

M. I. Afandi, N. N. (2021). Implementasi Algoritma Vigenere Cipher dan Atbash. *Informatic Tech. J.*, 30-41.

Nuniek Fahriani, I. K. (2021). Keamanan Data Pasien dengan Algoritma Blowfish pada HOTSPODT. *RISTEKDIKTI*, 1-9.

Susilo E.K, H. S. (2021). Monitoring RPM Engine dan Temperatur Minyak Pelumas pada Genset Berbasis IoT. *Jurnal Teknik Elektro dan Komputer*, 45-52.

Yoga Pratama, T. S. (2023). ANALISIS KRIPTOGRAFI ALGORITMA BLOWFISH PADA KEAMANAN DATA MENGGUNAKAN DART. *Jurnal Informatika Terpadu*, 1-10.

Yusril Agita Prayoga Tarigan, R. A. (2024). Algoritma AES 128 dalam Mengenkripsikan Berkas Bansos Kecamatan Tigabinanga Berbasis Web. *Jurnal Unitek*, 1-12.

Zaenul Arif, A. N. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi. *JTSI*, 1-12.