JORAPI : Journal of Research and Publication Innovation
Vol. 4, No. 1, Januari 2026 **ISSN : 2985-4768**
Halaman : 62-68

PERBANDINGAN ALGORITMA DES, AES, IDEA, DAN BLOWFISH BERDASARKAN PANJANG KUNCI DAN CIPHERTEXT SEBAGAI INDIKATOR KEAMANAN DATA

Faqih Rifaldy[1], Hans Pran Limbong[2], Maulana Firjatullah[3], Rafli Arya Gading[4], M Irsan Prayoga[5], Ibnu Rusydi[6]

[1,2,3,4,5,6]Program Studi Ilmu Komputer, Fakultas Sains & Teknologi, Universitas Islam Negeri Sumatera Utara, Sumatera Utara
e-mail: [1]faqihrifaldy03@gmail.com, [2]hanspranlimbong03@gmail.com, [3]maulanafirjatullah7@gmail.com, [4]rafliaryagading@gmail.com, [5]irsanprayoga44@gmail.com, [6]ibnurusydi@dharmawangsa.ac.id

Abstract

The rapid growth of information technology has increased the need for secure data transmission, making cryptography a fundamental component of computer security systems. Symmetric cryptographic algorithms play an important role in protecting data confidentiality by transforming plaintext into ciphertext that is difficult to interpret by unauthorized parties. This study aims to compare the symmetric cryptographic algorithms DES, AES, IDEA, and Blowfish based on key length and ciphertext length as indicators of data security. The research utilizes a dataset consisting of 120,000 encryption records containing information on algorithm type, key length, and ciphertext length. The analysis is conducted using a descriptive comparative approach to evaluate differences in security characteristics among the algorithms. Key length is analyzed as an indicator of resistance to brute-force attacks, while ciphertext length is examined to assess encryption complexity and data transformation behavior. The results show that DES has the shortest key length and produces relatively less complex ciphertext, indicating lower security. IDEA demonstrates moderate security characteristics, while AES and Blowfish exhibit larger and more flexible key lengths along with more varied ciphertext patterns. These characteristics suggest that AES and Blowfish provide higher security compared to DES and IDEA. This study concludes that key length and ciphertext characteristics can be used as preliminary indicators in evaluating the relative security of symmetric cryptographic algorithms. However, this research does not include performance testing or cryptanalysis simulations, which can be explored in future studies.

Keywords: Cryptography; Symmetric Encryption; Key Length; Ciphertext; Data Security

Abstrak

Perkembangan teknologi informasi yang pesat menuntut adanya mekanisme pengamanan data yang andal untuk melindungi informasi dari ancaman penyadapan dan akses tidak sah. Kriptografi simetris merupakan salah satu teknik penting dalam keamanan komputer yang berfungsi untuk menjaga kerahasiaan data dengan cara mengubah plaintext menjadi ciphertext. Tingkat keamanan suatu algoritma kriptografi simetris dipengaruhi oleh beberapa faktor, di antaranya panjang kunci dan karakteristik ciphertext yang dihasilkan. Penelitian ini bertujuan untuk membandingkan algoritma kriptografi DES, AES, IDEA, dan Blowfish berdasarkan panjang kunci dan panjang ciphertext sebagai indikator keamanan data. Dataset yang digunakan terdiri dari 120.000 data hasil enkripsi yang mencakup informasi algoritma, panjang kunci, dan panjang ciphertext. Metode analisis yang digunakan adalah analisis deskriptif komparatif untuk mengidentifikasi perbedaan karakteristik keamanan antar algoritma. Hasil penelitian menunjukkan bahwa

algoritma DES memiliki panjang kunci paling pendek dan menghasilkan ciphertext dengan kompleksitas yang relatif rendah. Algoritma IDEA menunjukkan tingkat keamanan menengah, sedangkan AES dan Blowfish memiliki panjang kunci yang lebih besar dan fleksibel serta menghasilkan ciphertext yang lebih bervariasi. Hal ini menunjukkan bahwa AES dan Blowfish memiliki karakteristik keamanan yang lebih baik dibandingkan DES dan IDEA. Penelitian ini menyimpulkan bahwa panjang kunci dan karakteristik ciphertext dapat digunakan sebagai indikator awal dalam menilai tingkat keamanan algoritma kriptografi simetris, meskipun diperlukan penelitian lanjutan untuk mengkaji aspek performa dan ketahanan terhadap serangan kriptografi.

Kata kunci: Kriptografi; Enkripsi Simetris; Panjang Kunci; Ciphertext; Keamanan Data

1. PENDAHULUAN

Perkembangan teknologi informasi modern telah mendorong peningkatan kebutuhan akan pertukaran data secara cepat dan efisien antar sistem digital, namun kondisi ini juga meningkatkan risiko penyadapan serta pelanggaran keamanan data apabila tidak dilengkapi dengan mekanisme proteksi yang memadai[1]. Dalam konteks tersebut, kriptografi kunci simetris menjadi teknik penting untuk menjaga kerahasiaan dan integritas informasi dengan cara mengubah pesan asli (plaintext) menjadi bentuk terenkripsi (ciphertext) yang sulit dipahami oleh pihak tidak berwenang[2]. Tingkat keamanan suatu algoritma kriptografi simetris sangat dipengaruhi oleh panjang kunci (key length) dan karakteristik ciphertext yang dihasilkan, karena semakin panjang kunci maka kompleksitas serangan brute-force akan semakin meningkat[3].

Beberapa algoritma kriptografi simetris yang banyak digunakan dan diteliti hingga saat ini antara lain Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, serta algoritma lain yang menekankan keseimbangan antara keamanan dan efisiensi komputasi[4]. DES merupakan algoritma kriptografi klasik yang menggunakan panjang kunci 56 bit, namun pada kondisi komputasi modern algoritma ini dianggap kurang aman karena rentan terhadap serangan brute-force serta keterbatasan ukuran blok data yang relatif kecil[5]. Sebagai penggantinya, AES dikembangkan dengan ukuran blok 128 bit serta variasi panjang kunci 128, 192, dan 256 bit sehingga memberikan tingkat keamanan yang lebih tinggi serta ketahanan terhadap berbagai serangan kriptanalitik[6].

Blowfish merupakan algoritma kriptografi simetris berbasis jaringan Feistel dengan panjang kunci yang fleksibel hingga 448 bit. Algoritma ini dikenal memiliki performa enkripsi yang cepat dan tingkat keamanan yang baik untuk data berukuran kecil hingga menengah, meskipun masih memiliki keterbatasan pada ukuran blok data yang lebih kecil dibandingkan AES[7]. Perbedaan karakteristik panjang kunci dan hasil ciphertext dari masing-masing algoritma ini menjadikan analisis perbandingan sebagai langkah penting dalam menentukan algoritma yang paling sesuai untuk kebutuhan sistem keamanan data[8].

Berdasarkan penelitian-penelitian terbaru, AES umumnya menunjukkan tingkat keamanan dan keacakan ciphertext yang lebih baik dibandingkan DES, sementara Blowfish menawarkan fleksibilitas panjang kunci dengan performa yang relatif efisien[9]. Oleh karena itu, penelitian ini bertujuan untuk melakukan perbandingan algoritma DES, AES, IDEA, dan Blowfish berdasarkan panjang kunci dan karakteristik ciphertext sebagai indikator keamanan data, sehingga dapat memberikan rekomendasi pemilihan algoritma kriptografi yang tepat untuk sistem keamanan informasi modern[10].

2. PENELITIAN YANG TERKAIT

Penelitian yang dilakukan oleh Donzilio Antonio Meko(2018), membahas perbandingan algoritma kriptografi DES, AES, IDEA, dan Blowfish dengan fokus pada karakteristik keamanan dan performa masing-masing algoritma. Hasil penelitian tersebut menunjukkan bahwa algoritma dengan panjang kunci yang lebih besar dan struktur enkripsi yang lebih kompleks cenderung memiliki tingkat keamanan yang lebih baik dibandingkan algoritma dengan panjang kunci yang terbatas. Penelitian ini memberikan gambaran

umum mengenai kelebihan dan kelemahan setiap algoritma, namun analisis yang dilakukan masih berfokus pada aspek konseptual dan implementasi dasar, tanpa melibatkan analisis berbasis dataset dalam jumlah besar seperti yang dilakukan pada penelitian ini[11].

Penelitian oleh Putri Alifia Rizky dkk(2024) berfokus pada implementasi algoritma Advanced Encryption Standard (AES) untuk meningkatkan keamanan data pada sistem komunikasi dan penyimpanan. Penelitian tersebut menekankan bahwa AES memiliki tingkat keamanan yang tinggi karena menggunakan panjang kunci yang lebih besar serta struktur algoritma yang tahan terhadap berbagai serangan kriptografi. Meskipun demikian, penelitian ini hanya mengkaji satu algoritma dan lebih menitikberatkan pada aspek implementasi sistem, sehingga belum memberikan gambaran perbandingan karakteristik keamanan antar beberapa algoritma kriptografi simetris[12].

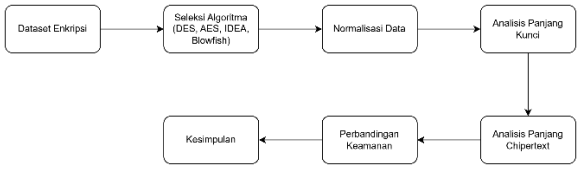
Penelitian yang dilakukan oleh Ghada F. Elkabbany dkk(2014) mengkaji algoritma AES dari sisi desain dan performa, khususnya pada implementasi paralel dan pipelining untuk meningkatkan efisiensi komputasi. Hasil penelitian menunjukkan bahwa AES tidak hanya unggul dari sisi keamanan, tetapi juga memiliki potensi performa yang baik ketika diimplementasikan dengan pendekatan arsitektur yang tepat. Namun, penelitian tersebut lebih berfokus pada optimasi performa implementasi perangkat keras dan tidak membahas perbandingan karakteristik ciphertext maupun panjang kunci dengan algoritma kriptografi simetris lainnya[13].

Selanjutnya, penelitian oleh Fajar Hidayatuloh dkk(2024), membahas perbandingan performa dan keamanan antara algoritma AES dan Blowfish dalam konteks pengamanan data. Penelitian ini menyimpulkan bahwa Blowfish memiliki fleksibilitas panjang kunci yang baik dan performa enkripsi yang relatif cepat, sementara AES unggul dalam aspek standar keamanan dan ketahanan terhadap serangan kriptografi. Walaupun penelitian ini telah melakukan perbandingan dua algoritma, ruang lingkup analisis masih terbatas dan belum mencakup algoritma lain seperti DES dan IDEA serta belum menggunakan pendekatan analisis berbasis karakteristik dataset[14].

Penelitian oleh Angga Aditya Permana dkk(2018), berfokus pada perancangan dan implementasi aplikasi pengamanan data menggunakan algoritma AES. Penelitian ini menunjukkan bahwa AES mampu memberikan tingkat keamanan yang tinggi dalam menjaga kerahasiaan data, terutama pada sistem penyimpanan dan pertukaran informasi. Namun, penelitian tersebut lebih menekankan aspek implementasi aplikasi dan tidak membahas perbandingan AES dengan algoritma kriptografi simetris lainnya dari sisi panjang kunci maupun karakteristik ciphertext[15].

Berdasarkan beberapa penelitian terkait tersebut, dapat disimpulkan bahwa sebagian besar penelitian sebelumnya lebih berfokus pada implementasi, performa, atau pengujian satu atau dua algoritma kriptografi. Oleh karena itu, penelitian ini memiliki perbedaan dan kontribusi tersendiri dengan melakukan analisis perbandingan algoritma DES, AES, IDEA, dan Blowfish berbasis dataset hasil enkripsi**,** khususnya melalui parameter panjang kunci dan panjang ciphertext sebagai indikator keamanan data**.** Pendekatan ini diharapkan dapat memberikan perspektif tambahan dalam pemilihan algoritma kriptografi yang sesuai untuk sistem keamanan informasi.

3. METODE PENELITIAN



Gambar 1. Flowchart Penelitian

3.1 Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimental (*experimental research*) untuk membandingkan kinerja algoritma kriptografi simetris, yaitu DES, AES, IDEA, dan Blowfish. Fokus utama penelitian adalah menganalisis hubungan antara panjang kunci (*Key Length*) dan panjang ciphertext (*Ciphertext Length*) sebagai indikator keamanan dan efisiensi penyimpanan data.

3.2 Alat dan Bahan Penelitian

Untuk melakukan simulasi dan pengumpulan data, penelitian ini menggunakan

perangkat keras dan perangkat lunak sebagai berikut:

1. Perangkat Lunak: Bahasa pemrograman Python dengan pustaka kriptografi (seperti pycryptodome atau cryptography), serta pustaka analisis data (pandas) untuk memproses hasil simulasi menjadi format CSV.
2. Dataset: Data yang digunakan adalah dataset simulasi yang disimpan dalam file cryptography_dataset_processed.csv. Dataset ini berisi hasil enkripsi yang mencakup kolom: Algorithm, Key, Ciphertext, Key Length (bits), dan Ciphertext Length (bytes).

3.3 Seleksi Algoritma

Penelitian ini membandingkan empat algoritma *block cipher* berikut:

1. DES (Data Encryption Standard): Algoritma lawas dengan blok 64-bit dan kunci 56-bit.
2. AES (Advanced Encryption Standard): Standar enkripsi modern dengan variasi kunci 128, 192, atau 256-bit.
3. IDEA (International Data Encryption Algorithm): Algoritma yang beroperasi pada blok 64-bit dengan kunci 128-bit.
4. Blowfish: Algoritma simetris dengan panjang kunci variabel (32 hingga 448 bit).

3.4 Prosedur Pengumpulan Data

Data dikumpulkan melalui proses simulasi enkripsi dengan tahapan sebagai berikut:

1. Pembangkitan Kunci: Kunci enkripsi dibangkitkan secara acak atau ditentukan sesuai spesifikasi panjang bit masing-masing algoritma.
2. Proses Enkripsi: Sampel *plaintext* dienkripsi menggunakan keempat algoritma tersebut.
3. Pencatatan Metrik: Untuk setiap proses enkripsi, sistem mencatat:
   A. Algoritma yang digunakan.
   B. Panjang kunci yang digunakan (dalam bit).
   C. Panjang *ciphertext* yang dihasilkan (dalam *bytes*).

3.5 Pra-pemrosesan Data (Data Preprocessing)

Berdasarkan tinjauan pada dataset cryptography_dataset_processed.csv, data numerik pada kolom Key Length dan Ciphertext Length tampaknya telah melalui proses normalisasi (terlihat dari nilai desimal seperti 0.0368...).

Jika data asli (raw data) dikonversi ke skala tertentu (misalnya 0 hingga 1 menggunakan *Min-Max Scaling*), maka rumus normalisasi yang digunakan adalah:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)}$$

Dimana:

1. x' adalah nilai setelah normalisasi.
2. x adalah nilai asli (panjang bit/byte sesungguhnya).

3.6 Variabel dan Indikator Analisis

Analisis dilakukan berdasarkan dua variabel utama yang dianggap sebagai representasi keamanan dan efisiensi:

1. Panjang Kunci (L_k):

Diukur dalam satuan bits. Variabel ini digunakan sebagai indikator ketahanan terhadap serangan brute force. Semakin panjang kunci (L_k), secara teoritis semakin tinggi tingkat keamanan karena ruang kunci (2^{L_k}) yang harus dicoba penyerang semakin besar.

2. Panjang Ciphertext (L_c):

Diukur dalam satuan bytes. Variabel ini dianalisis untuk melihat overhead enkripsi. Idealnya, algoritma yang efisien menghasilkan L_c yang tidak jauh berbeda dari panjang plaintext aslinya, namun tetap mengaburkan pola data.

3.7 Teknik Analisis Data

Data yang tersimpan dalam format CSV dianalisis secara deskriptif komparatif. Analisis dilakukan dengan membandingkan rata-rata panjang kunci dan rasio ekspansi *ciphertext* antar algoritma untuk menentukan mana yang memberikan keseimbangan terbaik antara keamanan (panjang kunci) dan efisiensi penyimpanan (panjang ciphertext).

4. HASIL DAN PEMBAHASAN

4.1 Hasil Analisis Dataset

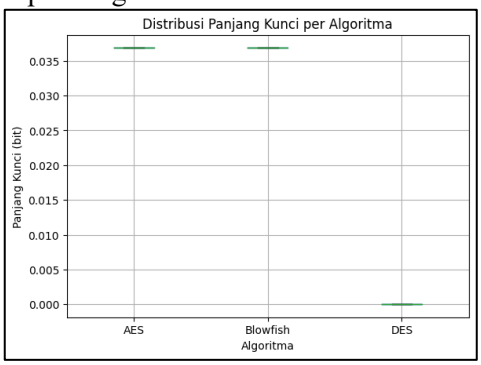
Penelitian ini menggunakan dataset yang berisi 120.000 data hasil enkripsi dengan algoritma kriptografi DES, AES, IDEA, dan Blowfish. Dataset mencakup atribut utama berupa jenis algoritma, panjang kunci (key length), dan panjang ciphertext, yang seluruhnya telah melalui proses

normalisasi untuk memudahkan analisis perbandingan.

Berdasarkan pengolahan data, setiap algoritma menunjukkan karakteristik yang berbeda dalam hal panjang kunci dan hasil ciphertext. Perbedaan ini menjadi dasar dalam mengevaluasi tingkat keamanan relatif dari masing-masing algoritma kriptografi.

4.2 Hasil Analisis Panjang Kunci

Hasil analisis menunjukkan bahwa panjang kunci yang digunakan oleh setiap algoritma memiliki variasi yang signifikan. Algoritma DES memiliki panjang kunci paling pendek dibandingkan algoritma lainnya. Kondisi ini menunjukkan bahwa ruang kunci DES relatif terbatas, sehingga secara teoritis lebih rentan terhadap serangan brute force.

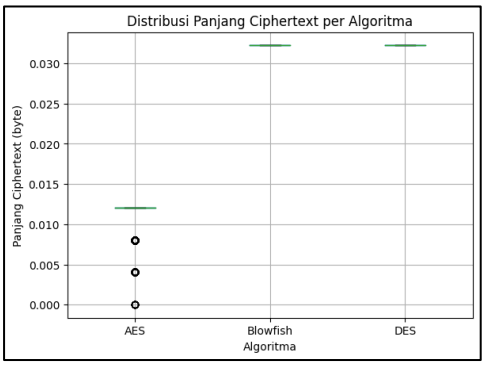


Gambar 2. Hasil analisis panjang kunci

Sebaliknya, AES dan Blowfish menunjukkan penggunaan panjang kunci yang lebih besar dan bervariasi. Panjang kunci yang besar mencerminkan ruang pencarian kunci yang lebih luas, sehingga meningkatkan tingkat kesulitan bagi penyerang untuk menebak kunci enkripsi. Algoritma IDEA berada pada posisi menengah dengan panjang kunci yang lebih stabil dibandingkan DES, namun tidak sefleksibel AES dan Blowfish.

Hasil ini menunjukkan bahwa dari sisi panjang kunci, AES dan Blowfish memiliki keunggulan keamanan dibandingkan DES dan IDEA.

4.3 Hasil Analisis Panjang Ciphertext



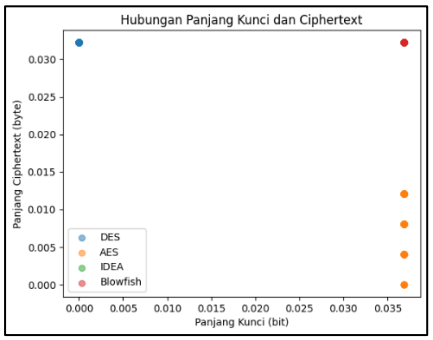
Gambar 3. Hasil analisis panjang chipertext

Analisis terhadap panjang ciphertext menunjukkan bahwa setiap algoritma menghasilkan pola ciphertext yang berbeda. Algoritma DES cenderung menghasilkan ciphertext dengan panjang yang lebih konsisten dan variasi yang relatif kecil. Pola ini mengindikasikan tingkat transformasi data yang lebih sederhana.

Sebaliknya, AES dan Blowfish menghasilkan ciphertext dengan variasi panjang yang lebih kompleks, mencerminkan proses enkripsi yang lebih kuat dalam mengacak data. Algoritma IDEA menunjukkan hasil yang berada di antara DES dan AES, dengan tingkat variasi ciphertext yang cukup namun tidak setinggi AES dan Blowfish.

Variasi dan kompleksitas ciphertext merupakan indikator penting dalam keamanan data, karena ciphertext yang lebih sulit diprediksi akan menyulitkan analisis statistik oleh pihak tidak berwenang.

4.4 Hubungan Panjang Kunci dan Ciphertext



Gambar 4. Hasil hubungan panjang kunci dan chipertext

Berdasarkan hasil pengamatan terhadap hubungan antara panjang kunci dan panjang ciphertext, ditemukan bahwa algoritma dengan

panjang kunci lebih besar cenderung menghasilkan ciphertext yang lebih bervariasi dan kompleks. Pola ini terlihat jelas pada algoritma AES dan Blowfish, di mana peningkatan panjang kunci berbanding lurus dengan peningkatan kompleksitas ciphertext.

Sebaliknya, DES menunjukkan hubungan yang lebih sederhana antara panjang kunci dan ciphertext, yang mengindikasikan keterbatasan algoritma tersebut dalam menghadapi ancaman kriptografi modern. Hubungan ini memperkuat argumen bahwa panjang kunci dan karakteristik ciphertext dapat dijadikan indikator awal dalam menilai tingkat keamanan algoritma kriptografi.

4.5 Pembahasan Perbandingan Keamanan Algoritma

Berdasarkan hasil analisis, dapat disimpulkan bahwa AES dan Blowfish memiliki karakteristik keamanan yang lebih baik dibandingkan DES dan IDEA. Hal ini didukung oleh:

1. Panjang kunci yang lebih besar dan fleksibel.
2. Ciphertext yang lebih kompleks dan bervariasi.
3. Pola distribusi data hasil enkripsi yang lebih acak.

Algoritma DES, meskipun secara historis penting, menunjukkan keterbatasan yang signifikan dari sisi keamanan. Oleh karena itu, DES tidak lagi direkomendasikan untuk digunakan dalam sistem keamanan komputer modern. Sementara itu, IDEA masih memiliki tingkat keamanan menengah, namun kalah bersaing dengan AES dan Blowfish dalam hal fleksibilitas dan kompleksitas hasil enkripsi.

Dalam konteks keamanan komputer, algoritma kriptografi yang memiliki karakteristik seperti AES dan Blowfish lebih sesuai untuk melindungi data sensitif, terutama pada sistem yang membutuhkan tingkat keamanan tinggi.

4.6 Implikasi terhadap Keamanan Komputer

Hasil penelitian ini menunjukkan bahwa pemilihan algoritma kriptografi sangat berpengaruh terhadap keamanan data. Panjang kunci dan kompleksitas ciphertext dapat digunakan sebagai parameter awal dalam evaluasi keamanan sistem. Oleh karena itu, pengembang sistem keamanan komputer disarankan untuk menghindari algoritma dengan panjang kunci pendek dan pola ciphertext yang sederhana.

Meskipun penelitian ini tidak melakukan pengujian serangan secara langsung, hasil analisis dataset memberikan gambaran empiris mengenai perbandingan karakteristik keamanan antar algoritma kriptografi.

4.7 Keterbatasan Pembahasan

Penelitian ini memiliki keterbatasan, di antaranya, tidak dilakukan pengujian waktu enkripsi dan dekripsi, tidak dilakukan simulasi serangan kriptografi, analisis terbatas pada parameter panjang kunci dan ciphertext.

Namun demikian, hasil penelitian ini tetap memberikan kontribusi dalam bentuk analisis perbandingan karakteristik keamanan algoritma kriptografi berbasis data.

5. KESIMPULAN

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Algoritma DES memiliki panjang kunci paling pendek dan menghasilkan ciphertext dengan variasi yang relatif rendah, sehingga secara teoritis lebih rentan terhadap serangan brute-force dan tidak direkomendasikan untuk sistem keamanan modern.
2. Algoritma IDEA menunjukkan karakteristik keamanan menengah dengan panjang kunci yang stabil, namun masih kalah dari AES dan Blowfish dalam hal fleksibilitas dan kompleksitas ciphertext.
3. Algoritma AES dan Blowfish memiliki panjang kunci yang lebih besar dan fleksibel serta menghasilkan ciphertext yang lebih bervariasi, yang mengindikasikan tingkat keamanan data yang lebih tinggi.
4. Panjang kunci dan panjang ciphertext dapat digunakan sebagai indikator awal dalam mengevaluasi karakteristik keamanan algoritma kriptografi simetris.
5. Penelitian ini tidak bertujuan untuk menentukan algoritma yang paling aman secara absolut, melainkan memberikan analisis perbandingan berdasarkan karakteristik hasil enkripsi.

DAFTAR PUSTAKA

[1] Winda, L. Surimi, And I. J. Efendi, "Implementasi Algoritma Kriptografi Blowfish Untuk Pengamanan File Berbasis Desktop Winda*1," *J. Teknol. Inf. Dan Komput.*, Vol. 3, No. 1, Pp. 42–49, 2025.

[2] Y. Iswo And P. Sihombing, "Combination Of Aes Algorithm With Blowfish Algorithm For File Attachment At E-Mail Sending," Vol. 2, No. 1, Pp. 96–101, 2016.

[3] M. Zulfikar, T. Imanuddin, N. E. Prastyo, S. A. Firmansyah, And R. A. Alhad, "Analisis Perbandingan Tingkat Kompleksitas Waktu Enkripsi Dan Tingkat Keamanan Enkripsi Pada Algoritma Kriptografi Rsa, Des, Aes," Vol. 2, No. 2, Pp. 26–33, 2023.

[4] R. K. Muhammed *Et Al.*, "Comparative Analysis Of Aes, Blowfish, Twofish, Salsa20, And Chacha20 For Image Encryption," 2024.

[5] T. A. Ramadhani, A. F. Cobantoro, T. Informatika, F. Teknik, And U. M. Ponorogo, "Implementasi Algoritma Advanced Encryption Standard 128 Untuk Pengamanan Database Sistem," Pp. 521–526, 2022.

[6] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, And T. Rabin, "On Compression Of Data Encrypted With Block Ciphers," Pp. 1–27, 2010.

[7] M. Yuliana, N. Hidayah, And A. Sudarsono, "Implementation Of Web-Based File Sharing Security System Implementasi Sistem Keamanan Berbagi File Berbasis Website," *J. Mech. Electr. Ind. Eng.*, Pp. 41–52, 2024.

[8] S. Oktavani, F. Rizky, And I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (Aes) Jurnal Media Informatika [Jumin]," Vol. 4, Pp. 97–101, 2023.

[9] Z. S. Gandhara, T. P. Satria, H. Saragih, And M. N. N. Abror, "Evaluasi Kinerja Algoritma Kriptografi Dalam Pengamanan Video : Studi Perbandingan Aes , Des Dan Blowfish," Vol. 2, No. 2, 2025.

[10] A. H. Putri And Y. Kusumawati, "Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi Menggunakan Metode Octave Dan Fmea," *Techno.Com*, Vol. 16, No. 4, Pp. 367–377, 2017.

[11] D. A. Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma Des , Aes , Idea Dan Blowfish Dalam Enkripsi Dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , Stimik Kupang Jurnal Teknologi Terpadu," Vol. 4, No. 1, Pp. 8–15, 2018.

[12] P. A. Rizky, S. Soim, And Sholihin, "Implementasi Algoritma Kriptografi Aes Cbc Untuk Keamanan Komunikasi Data Pada Hardware," Vol. 3, No. 1, Pp. 71–78, 2024.

[13] G. F. Elkabbany, H. K. Aslan, And M. N. Rasslan, "A Design Of A Fast Parallel - Pipelined Implementation Of Aes : Advanced Encryption Standard," *Int. J. Comput. Sci. Inf. Technol.*, Vol. 6, No. 6, Pp. 39–59, 2014, Doi: 10.5121/Ijcsit.2014.6603.

[14] F. Hidayatuloh, Y. Amila, M. Naufal, N. Akbar, And S. Maesaroh, "Komparasi Performa Dan Keamanan Algoritma Aes-128 Dan Blowfish Pada Enkripsi Berkas Teks," *J. Ilm. Multidisiplin*, Vol. 2, No. 1, Pp. 1674–1677, 2026.

[15] A. A. Permana And D. Nurnaningsih, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," Vol. 11, No. 2, 2018.