

Analisis Komparatif Algoritma AES, Blowfish dan Pendekatan *Hybrid* untuk Menjaga Kerahasiaan Dokumen Pengadilan Agama

Hasda Nuril Mala^{*1}, Eko Riyanto², Sri Lestari Ratna Anugraheni³, Eka Ardhianto⁴, Aji Supriyanto⁵

^{1,2}Pengadilan Tinggi Agama Semarang, Mahkamah Agung, Indonesia

^{3,4,5}Program Studi Teknologi Informasi, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank, Indonesia

Email: ¹hasda.nm28@gmail.com, ²ekoriyanto0027@mhs.unisbank.ac.id,

³srilestari0003@mhs.unisbank.ac.id, ⁴ekaardhianto@edu.unisbank.ac.id, ⁵ajisup@edu.unisbank.ac.id

Abstrak

Keamanan dokumen digital menjadi aspek penting dalam menjaga kerahasiaan informasi, khususnya pada dokumen berbasis PDF. Penelitian ini bertujuan untuk menganalisis dan membandingkan performa algoritma kriptografi AES, *Blowfish* dan metode *hybrid* yang merupakan gabungan antara AES dan *Blowfish* dalam mengamankan dokumen yang ada di lingkungan pengadilan agama. Pada penelitian ini, menggunakan 6 dokumen dengan kisaran ukuran 261 KB - 1,7 MB serta proses enkripsi dan dekripsi dilakukan sebanyak 5 kali iterasi untuk memperoleh hasil yang konsisten. Adapun parameter evaluasi yang digunakan meliputi waktu eksekusi enkripsi dan dekripsi, entropi dan *avalanche effect*. Hasil penelitian menunjukkan bahwa AES memiliki performa terbaik dalam segi kecepatan dengan rata-rata waktu enkripsi selama 0,078 ms dan dekripsi selama 0,052 ms, yang merupakan nilai terendah dibandingkan *Blowfish* dan *hybrid* yang rata-rata waktu enkripsinya mencapai 0,554 ms. Sedangkan dari segi keamanan ketiga pendekatan tersebut menghasilkan nilai entropi yang tinggi dan relatif sama. Namun, pada hasil *avalanche effect*, *hybrid* menghasilkan nilai tertinggi mencapai 0,153, lebih unggul dibandingkan AES dan *Blowfish*. Dengan demikian, AES lebih unggul dalam efisiensi waktu, sedangkan *hybrid* lebih unggul dalam aspek keamanan.

Kata kunci: *advance encryption standard, avalanche effect, blowfish, digital document, entropy, symmetric key cryptography.*

Abstract

The security of digital documents is a critical concern in preserving information confidentiality, particularly for PDF-based documents in sensitive environments such as religious courts. This study presents a comparative analysis of three cryptographic approaches: AES, *Blowfish* and a hybrid method combining AES and *Blowfish* for document protection. A total of 6 documents with file sizes ranging from 261 KB to 1,7 MB were used in the experiments and the encryption-decryption processes were repeated five times to ensure result consistency. Performance evaluation was conducted using three key parameters: execution time, entropy and *avalanche effect*. The results show that AES achieves the best performance in terms of computational efficiency, with the lowest average encryption time of 0,078 ms and decryption time of 0,052 ms, which are lower compared to *blowfish* and the hybrid method, where the average encryption time reaches 0,554 ms. In contrast, all three approaches exhibit high and comparable entropy values. However, the hybrid method demonstrates superior performance in *avalanche effect*, reaching the highest value of 0,153. These findings suggest that AES is more suitable for applications requiring high efficiency, whereas the hybrid approach is preferable for scenarios demanding enhanced security.

Keywords: *advance encryption standard, avalanche effect, blowfish, digital document, entropy, symmetric key cryptography.*

This work is an open access article and licensed under a Creative Commons Attribution-NonCommercial ShareAlike 4.0 International (CC BY-NC-SA 4.0)



1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam pengelolaan dan distribusi dokumen digital, termasuk lingkungan lembaga peradilan. Pengadilan Agama merupakan salah satu institusi peradilan di Indonesia yang mengelola berbagai dokumen penting seperti dokumen

permohonan atau gugatan, berkas persidangan, dokumen putusan, dan dokumen administrasi lainnya yang bersifat rahasia. Dalam konteks ini, dokumen yang dikelola tidak hanya bersifat administratif, tetapi juga mengandung data pribadi dan informasi sensitif yang harus dilindungi dari potensi kebocoran maupun akses yang tidak sah. Oleh karena itu, diperlukan mekanisme pengamanan informasi yang mampu menjaga kerahasiaan dokumen-dokumen tersebut dari akses yang tidak sah. Kebutuhan ini juga sejalan dengan amanat Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang menekankan pentingnya perlindungan data pribadi melalui penerapan prinsip keamanan dan kerahasiaan dalam pengelolaan data. Dalam konteks ini, peradilan sebagai instansi pemerintah dituntut untuk menerapkan pengamanan data dan informasi yang memadai guna mencegah kebocoran atau penyalahgunaan data. Salah satu pendekatan yang telah lama digunakan dalam menjaga keamanan atau kerahasiaan informasi/dokumen adalah kriptografi. Kriptografi sendiri merupakan teknik untuk melindungi informasi dengan mengubah informasi ke dalam bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang atau tidak memiliki izin [1].

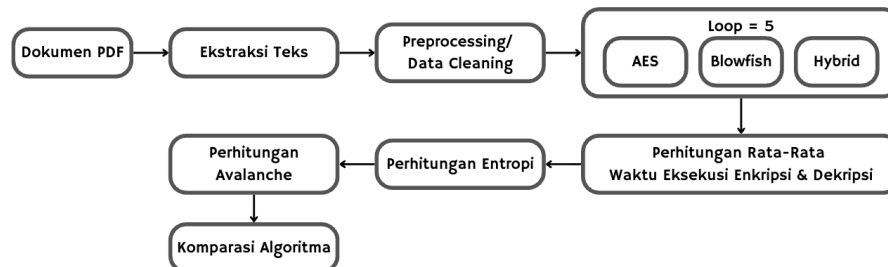
Seiring perkembangan teknologi, metode kriptografi juga mengalami pergeseran dari proses enkripsi manual ke mesin kriptografi yang secara signifikan meningkatkan kompleksitas kriptografi [2]. Kriptografi modern yang dipicu oleh perkembangan peralatan komputer digital sangat memungkinkan untuk menghasilkan *cipher* yang lebih kompleks. Berbeda hal dengan kriptografi klasik yang mengenkripsi karakter per-karakter (dengan menggunakan alfabet tradisional), sedangkan kriptografi modern beroperasi pada *string biner*. Kriptografi memiliki dua fungsi utama yaitu fungsi enkripsi yang merupakan proses mengubah pesan (*plaintext*) menjadi format yang tidak dapat dibaca (*ciphertext*), dan fungsi dekripsi yang merupakan proses mengembalikan pesan terenkripsi (*chipertext*) menjadi bentuk aslinya yang dapat dipahami (*plaintext*) [3]. Berdasarkan jenis kunci (*key*) yang digunakan, kriptografi modern terbagi menjadi dua yakni kriptografi simetris (*symmetric key cryptography*) yang menggunakan satu kunci rahasia yang sama untuk proses enkripsi dan dekripsinya, seperti algoritma DES (*Data Encryption Standard*), AES (*Advance Encryption Standard*), *Twofish* dan *Blowfish*. Selanjutnya ada juga kriptografi asimetris (*asymmetric key cryptography*) yang memanfaatkan sepasang kunci yaitu *public key* dan *private key* untuk menjaga keamanan data, seperti RSA (Rivest, Shamir, and Adleman) [2], [3].

Secara spesifik, penelitian ini berfokus pada analisis hasil implementasi dan perbandingan dua algoritma dan satu metode yakni AES, *Blowfish* dan *hybrid*. AES dan *Blowfish* dipilih karena keduanya dikenal sebagai algoritma kriptografi simetris yang kuat dan andal [4], [5], sedangkan kriptografi simetris sendiri, menurut [6] dan diperkuat oleh [7], merupakan kriptografi yang menonjol dalam hal efisiensi dan kecepatan, sehingga menjadikannya pilihan unggul untuk mengenkripsi *volume* data besar seperti *file*. Namun demikian, setiap algoritma memiliki karakteristik yang berbeda, baik dari segi waktu eksekusi saat enkripsi dan dekripsi, maupun tingkat keamanan yang dihasilkan. Perbedaan ini menimbulkan tantangan dalam menentukan metode yang paling optimal untuk menjamin keamanan dokumen tanpa mengorbankan performa sistem. Meskipun berbagai penelitian telah mengkaji performa AES dan *Blowfish*, sebagian besar studi masih berfokus pada perbandingan kecepatan dan keamanan secara terpisah tanpa mengeksplorasi keduanya. Sebagaimana pada studi yang dilakukan oleh [8] yang menunjukkan bahwa AES lebih unggul dalam efisiensi waktu dibandingkan *Blowfish*, sementara pada studi lain menegaskan bahwa kedua algoritma memiliki tingkat keamanan yang tinggi berdasarkan panjang kunci dan karakteristik *ciphertext* yang dihasilkan [9]. Namun demikian, studi yang menggabungkan kedua algoritma tersebut dalam satu skema pengamanan, khususnya pada dokumen pengadilan agama yang memiliki tingkat sensitivitas tinggi masih relatif terbatas. Di sisi lain, pendekatan *hybrid* yang menggabungkan AES dan *Blowfish* menawarkan potensi peningkatan keamanan melalui skema enkripsi berlapis, tetapi juga berimplikasi pada kompleksitas dan waktu eksekusi. Oleh karena itu, diperlukan evaluasi dan komparasi yang komprehensif terhadap AES, *Blowfish* dan metode *hybrid* berdasarkan parameter waktu eksekusi saat enkripsi dan dekripsi, nilai entropi serta *avalanche effect*, guna mengidentifikasi metode yang paling efektif dan efisien dalam mendukung pengamanan dokumen pengadilan agama.

2. METODE PENELITIAN

Penelitian dalam studi ini merupakan penelitian eksperimen kuantitatif yang bertujuan untuk mengevaluasi performa dan tingkat keamanan algoritma kriptografi melalui pengujian terkontrol

menggunakan beberapa parameter terukur. Sebagaimana pada Gambar 1, penelitian ini diawali dengan pengumpulan data berupa Dokumen PDF. Adapun dokumen yang digunakan dalam penelitian ini merupakan dokumen permohonan dan gugatan yang ada di Pengadilan Agama dengan dua karakteristik, yakni dokumen dengan *size* dokumen < 1 MB dan 1 MB < *size* dokumen < 2 MB. Selanjutnya, dilakukan proses ekstraksi teks untuk mengubah isi dokumen PDF menjadi data teks mentah yang dapat diolah lebih lanjut.



Gambar 1. Alur kerja penelitian

Teks hasil ekstraksi kemudian dilakukan pembersihan data (*preprocessing*) untuk menghilangkan simbol karakter aneh, karakter *non-printable* hasil ekstraksi dan menghilangkan spasi yang berlebihan pada teks. Selanjutnya data yang sudah dibersihkan mulai diproses enkripsi-dekripsi dengan menggunakan tiga pendekatan yaitu AES, *Blowfish* serta gabungan antara AES dan *Blowfish* (*hybrid*). Implementasi ketiga pendekatan tersebut dilakukan menggunakan *library* PyCryptodome dalam bahasa pemrograman *python* pada perangkat dengan spesifikasi sebagai berikut:

- Operasi sistem : macOS Tahoe 26.2,
- Chipset* : Apple M4 (10 *core* CPU 10 *core* GPU),
- Memory/Storage* : LPDDR5 24 GB, SSD 512 GB.

Pengujian performa untuk waktu eksekusi proses enkripsi dan dekripsi dilakukan sebanyak lima kali perulangan untuk memastikan konsistensi dan akurasi hasil. Selain itu, dilakukan juga dua pengujian untuk ketiga pendekatan, yakni terdiri dari uji entropi dan uji *avalanche effect*. Uji entropi dilakukan untuk menilai kekuatan hasil enkripsi dengan cara mengukur seberapa acak dan kuat *ciphertext* tersebut, dalam penelitian ini menggunakan *Shannon entropy*. Sedangkan uji *avalanche effect* untuk mengetahui sensitifitas perubahan *output* terhadap perubahan kecil pada *input*.

2.1. Ekstraksi Teks

Proses ekstraksi teks dalam penelitian ini mengadopsi pendekatan hirarki (*hierarchical approach*), dimana beberapa metode ekstraksi diterapkan secara bertingkat berdasarkan evaluasi hasil pada setiap tahap. Tahap awal menggunakan PyPDF2 untuk mengekstraksi teks secara langsung dari dokumen. Apabila hasil yang diperoleh belum memadai, proses dilanjutkan menggunakan pdfplumber yang lebih adaptif terhadap struktur dokumen yang kompleks. Selanjutnya, jika kedua metode tersebut belum menghasilkan teks yang optimal, digunakan pendekatan OCR (*Optical Character Recognition*) untuk mengekstraksi teks dari dokumen berbasis citra. Pendekatan ini memungkinkan peningkatan *robustness*, akurasi, dan kelengkapan hasil ekstraksi pada berbagai karakteristik dokumen PDF.

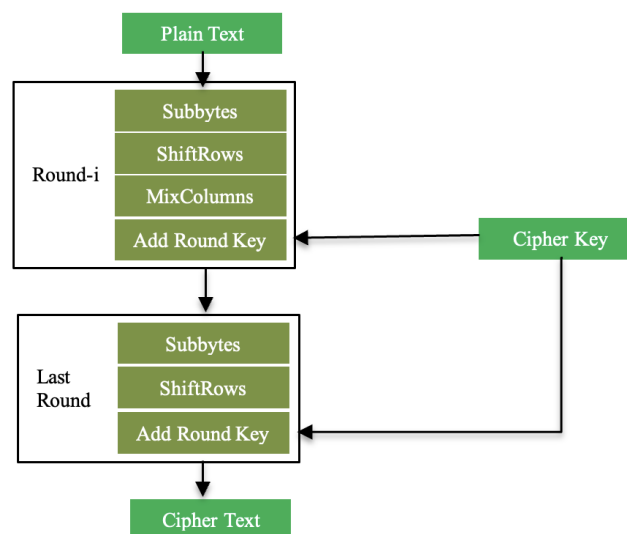
2.2. Preprocessing

Pada tahapan ini melibatkan proses normalisasi teks yang berfungsi untuk membersihkan data dari *noise* yang dihasilkan selama proses ekstraksi, khususnya dari metode OCR. Adapun proses yang dilakukan antara lain:

- Mengganti nilai kosong (*null*) dengan *string* kosong,
- Mengubah tipe data menjadi *string*,
- Mengganti semua pola spasi berulang dengan satu spasi,
- Mengganti karakter di luar ASCII *printable* dengan spasi, dan
- Menghapus spasi di awal dan akhir teks.

2.3. Advance Encryption Standard

AES atau dikenal juga sebagai algoritma Rijndael, dibuat oleh Vincent Rijmen dan Joan Daeman yang dipilih oleh NIST sebagai standar enkripsi pada tahun 2001 [10]. Enkripsi dan dekripsi AES dikatakan 3x lebih cepat dan lebih aman dibandingkan dengan DES [2]. AES sendiri dirancang untuk menggantikan DES yang dianggap tak lagi aman terhadap serangan *brute-force* [10]. Berdasarkan panjang kuncinya, AES dibagi menjadi AES 128-bit, AES 192-bit, dan AES 256-bit. Beberapa konfigurasi lain pada AES antara lain mode *chaining* (seperti ECB, CBC, dsb) dan mode *padding* (seperti Zero, PKCS7). Enkripsi AES ini terdiri beberapa *round* yang setiap *round* dirancang untuk meningkatkan keamanan melalui serangkaian transformasi. Dalam setiap *round*-nya juga melibatkan empat tahap utama antara lain *AddRoundKey*, yaitu menggabungkan data dengan kunci menggunakan operasi XOR, *SubBytes*, mengganti setiap *byte* menggunakan S-Box untuk meningkatkan ketidakpastian, *ShiftRows*, menggeser baris data secara melingkar untuk mendistribusikan ulang *byte* dan *MixColumns*, yaitu mencampur *byte* dalam setiap kolom untuk semakin menyamarkan pola data [7], [11].



Gambar 2. Proses enkripsi AES

Konfigurasi AES yang digunakan dalam penelitian ini menggunakan mode CBC (*Chiper Block Chaining*) dengan mekanisme *padding* PKCS7 untuk memastikan panjang blok sesuai dengan ukuran blok AES 16 *byte*. Berdasarkan skema AES pada Gambar 2, algoritma AES yang digunakan, secara garis besar disajikan pada Tabel 1.

Tabel 1. *Pseudocode* AES

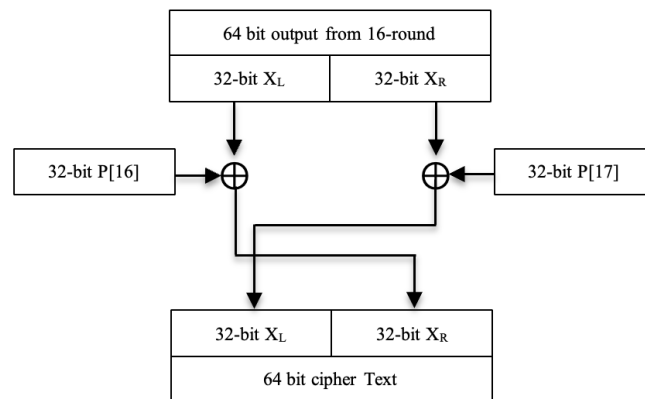
Input	: dataset dokumen (df), password, iterasi
Output	: encrypt_time, decrypt_time
Prosedur	: a. Mulai b. Bangkitkan kunci: - aes_key ← SHA-256 (password) ambil 16 byte c. Bangkitkan aes_iv (16 byte) d. Untuk setiap dokumen pada dataset: • Ambil text_clean dan nama dokumen e. Ulangi iterasi: • Enkripsi AES-CBC → ciphertext • Dekripsi AES-CBC → plaintext f. Hitung rata-rata waktu enkripsi g. Hitung rata-rata waktu dekripsi

2.4. Blowfish

Blowfish pertama kali diperkenalkan pada tahun 1993 oleh seorang kriptografer bernama Bruce Schneier. Merupakan algoritma yang digunakan secara bebas, gratis, tidak memerlukan lisensi dan tidak memiliki paten [2]. Algoritma ini memiliki dua komponen utama yang terdiri dari *key expansion* dan *data encryption*.

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, pada *data encryption* inilah terjadi iterasi sebanyak 16 *round*, dengan setiap bloknnya berukuran 64-bit dengan struktur Feistel *network* [8].

Setiap *round* terdiri dari dua operasi yaitu permutasi dan *key-dependent substitution*. Operasi permutasi yang digunakan tidak bergantung pada kunci dan begitu pula dengan operasi substitusi yang tidak bergantung pada data maupun kunci secara langsung. Adapun operasi dasar yang digunakan mencakup modulo serta XOR terhadap *word* 32-bit, disertai akses terhadap 4 indeks *array* (*lookup table*) pada setiap *round*. *Blowfish* dalam penelitian ini diimplementasikan dengan skema proses yang berbeda, sebagaimana ditunjukkan pada Gambar 3.



Gambar 3. Proses enkripsi *Blowfish*

Blowfish dalam penelitian ini bekerja dengan ukuran blok 64-bit dan mendukung panjang kunci yang bervariasi. Secara garis besar, algoritma *Blowfish* yang digunakan dalam penelitian ini disajikan dalam Tabel 2.

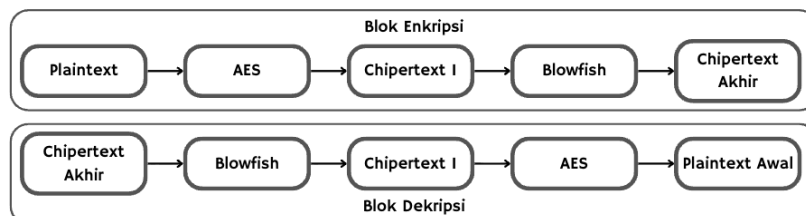
Tabel 2. *Pseudocode Blowfish*

Input	: dataset dokumen (df), password, iterasi
Output	: encrypt_time, decrypt_time
Prosedur	: a. Mulai b. Bangkitkan kunci: - bf_key ← SHA-256 (password) ambil 16 byte c. Bangkitkan bf_iv (8 byte) d. Untuk setiap dokumen pada dataset: • Ambil text_clean dan nama dokumen e. Ulangi iterasi: • Enkripsi Blowfish-CBC → ciphertext • Dekripsi Blowfish-CBC → plaintext f. Hitung rata-rata waktu enkripsi g. Hitung rata-rata waktu dekripsi

2.5. Pendekatan Hybrid

Pendekatan *hybrid* pada penelitian ini merupakan metode yang mengombinasikan antara algoritma AES dan *Blowfish*, dalam skema ini proses enkripsi dan dekripsi dilakukan secara berlapis (*sequential encryption*) sebagaimana pada Gambar 4. Berbeda dengan kriptografi *hybrid* yang umumnya

mengintegrasikan algoritma secara paralel atau melalui pembagian fungsi tertentu, metode dalam penelitian ini menerapkan proses enkripsi secara bertahap. Proses enkripsi yang terjadi yaitu dari *plaintext* menggunakan AES terlebih dahulu kemudian hasilnya dienkripsi kembali menggunakan *Blowfish*.



Gambar 4. Skema pendekatan *hybrid*

Begitu pula pada proses dekripsinya, dari *ciphertext* akhir didekripsi menggunakan *Blowfish* terlebih dahulu kemudian hasilnya didekripsi lagi menggunakan AES untuk memperoleh *plaintext* awal. Adapun *key* yang digunakan dalam penelitian ini antara AES dan *Blowfish* sebagaimana ditunjukkan pada Tabel 1 dan Tabel 2, keduanya menggunakan sumber *password* yang sama dan masing-masing membangkitkan *key* menggunakan fungsi *hash* SHA-256, dengan 16 *byte* pertama dari hasil *hash* digunakan sebagai *key* pada kedua algoritma. Meskipun secara teoritis *Blowfish* mendukung panjang *key* hingga 56 *byte*, namun penelitian ini menggunakan *key* dengan panjang 16 *byte* untuk menjaga konsistensi konfigurasi pada seluruh eksperimen.

2.6. Evaluasi Keamanan

Keamanan merupakan salah satu aspek yang sangat penting dalam sistem kriptografi untuk memastikan bahwa algoritma yang digunakan mampu melindungi data dari berbagai serangan khususnya analisis statistik dan kriptanalisis. Parameter yang umum digunakan dalam mengukur tingkat keamanan algoritma kriptografi adalah entropi dan *avalanche effect*.

Salah satu entropi yang umum digunakan adalah *Shannon entropy*, digunakan untuk mengukur tingkat ketidakpastian informasi atau keacakan (*randomness*) distribusi *byte* dalam *ciphertext* [12]. Entropi ini dihitung menggunakan rumus standar entropi:

$$entropi = - \sum_{i=1}^n p(x_i) \log_2 p(x_i) \quad (1)$$

Dimana n adalah jumlah total simbol unik (256 kemungkinan untuk satu *byte*) dan $p(x_i)$ adalah probabilitas kemunculan *byte* ke- i dalam *stream* data. Kunci kriptografi yang baik harus memiliki distribusi bit yang seragam, sehingga nilai entropinya mendekati batas maksimum yaitu 8.0 bit/*byte* [13]. Semakin dekat nilai H ke 8 maka akan semakin sulit pula pola kunci diprediksi.

Parameter ke-2 adalah *avalanche effect*, pertama kali diperkenalkan pada tahun 1985 oleh Webster dan Taveres [14]. Parameter ini menjadi salah satu faktor yang paling esensial yang perlu diperhatikan ketika mengevaluasi kekuatan algoritma kriptografi. Pengujian parameter ini menekankan modifikasi kecil pada satu bit data ASCII baik pada *plaintext* maupun *ciphertext*, yang akan menyebabkan perubahan signifikan pada *output ciphertext* [15]. Adapun perhitungan yang digunakan adalah sebagaimana pada persamaan berikut:

$$avalanche = \frac{\text{perubahan bit}}{\text{total bit}} \times 100\% \quad (2)$$

Pada parameter ini, semakin besar perubahan bit yang terjadi pada *ciphertext* akibat perubahan kecil pada *plaintext*, maka akan semakin baik tingkat difusi algoritma kriptografi dan semakin sulit pola *ciphertext* diprediksi. Pengujian *avalanche effect* pada penelitian ini dilakukan dengan menerapkan perubahan minimal pada *plaintext* awal melalui substitusi satu karakter pada posisi akhir teks. Meskipun tidak menggunakan teknik *one-bit flipping* secara eksplisit, pendekatan ini tetap menghasilkan perubahan pada representasi biner *plaintext* karena setiap karakter direpresentasikan dalam bentuk *byte*. Berbeda dengan evaluasi waktu eksekusi yang dilakukan sebanyak lima kali pada setiap dokumen, evaluasi keamanan melalui entropi dan *avalanche effect* ini dilakukan satu kali untuk setiap dokumen.

3. HASIL DAN PEMBAHASAN

Dokumen PDF yang akan dienkrpsi dengan karakteristik yang telah diuraikan pada bab sebelumnya, terlebih dahulu diekstraksi kemudian dilakukan pembersihan teks (*data cleaning*).

Tabel 3. Karakteristik Data yang Digunakan

Dokumen	Size	Panjang Teks	
		Hasil Ekstrak	Preprocessing
G-1189	1.7 MB	8227	8165
G-694	1.3 MB	7653	7624
G-358	1.4 MB	25183	24975
P-355	261 KB	5694	5546
P-360	704 KB	6700	6595
P-104	606 KB	6283	6145

Setelah dilakukan *data cleaning*, panjang teks dari hasil ekstraksi secara otomatis mengalami perubahan (cenderung mengalami penurunan) jumlah panjang teks sebagaimana pada Tabel 3.

3.1. Analisis Waktu Eksekusi Enkripsi - Dekripsi

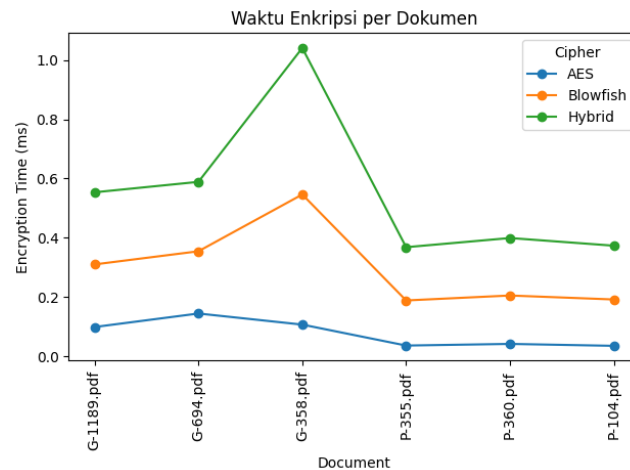
Berdasarkan hasil pengujian sebagaimana pada Tabel 4, algoritma AES menunjukkan kinerja paling optimal dalam hal waktu eksekusi, dengan rata-rata waktu enkripsi sebesar 0,078 ms dan dekripsi sebesar 0,052 ms. Hal ini menunjukkan bahwa AES memiliki efisiensi komputasi yang tinggi. Sebaliknya, algoritma *Blowfish* membutuhkan waktu yang lebih lama, yaitu 0,300 ms untuk proses enkripsi dan sebesar 0,238 ms untuk proses dekripsi. Perbedaan ini menunjukkan bahwa *Blowfish* memiliki kompleksitas proses yang lebih tinggi dibandingkan AES dalam implementasi yang digunakan.

Metode *hybrid* yang merupakan gabungan antara AES dan *Blowfish* mencatat waktu eksekusi paling lama, dengan enkripsi selama 0,554 ms dan proses dekripsi selama 0,461 ms. Hal ini disebabkan oleh penggunaan dua algoritma secara berlapis, sehingga proses komputasi menjadi lebih kompleks.

Tabel 4. Komparasi Rata-Rata Waktu Eksekusi Enkripsi & Dekripsi

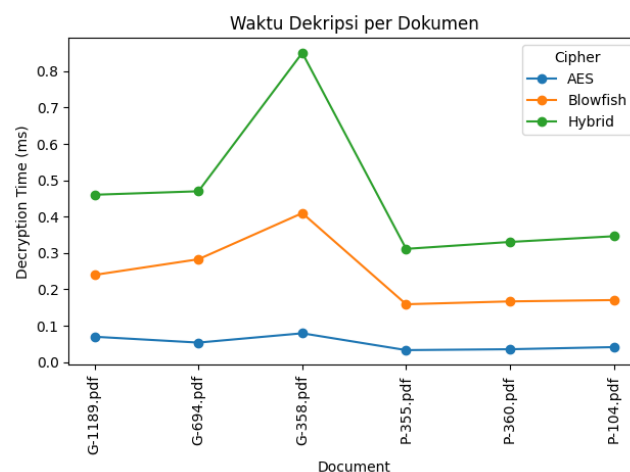
Algoritma	Enkripsi (ms)	Dekripsi (ms)
AES	0.078	0.052
<i>Blowfish</i>	0.300	0.238
<i>Hybrid</i> (AES + <i>Blowfish</i>)	0.554	0.461

Dengan demikian, dapat disimpulkan bahwa terdapat *trade-off* antara kompleksitas metode dan efisiensi waktu, dimana semakin kompleks algoritma yang digunakan maka semakin besar waktu yang dibutuhkan. Hal ini sejalan dengan grafik waktu eksekusi proses enkripsi dan dekripsi pada tiap dokumen yang dapat dilihat pada Gambar 5 dan Gambar 6.



Gambar 5. Waktu eksekusi enkripsi pada tiap dokumen

Pada grafik enkripsi, algoritma AES (garis biru) secara konsisten berada pada posisi paling rendah di seluruh dokumen, yang menunjukkan waktu eksekusi paling cepat dibandingkan dua algoritma lainnya. *Blowfish* (garis oranye) berada pada posisi tengah sedangkan *hybrid* (garis hijau) berada di bagian paling tinggi, yang menandakan waktu eksekusi enkripsinya paling lama.



Gambar 6. Waktu eksekusi dekripsi pada tiap dokumen

Pada grafik dekripsi, pola yang sama juga terlihat dengan tren yang hampir identik. AES kembali menunjukkan performa tercepat dengan waktu dekripsi yang sangat rendah dan stabil di semua dokumen. *Blowfish* menunjukkan waktu yang lebih tinggi namun masih relatif stabil dan lebih rendah dibanding *hybrid* yang pada grafik di Gambar 5 menunjukkan performa yang paling lambat.

Selain itu, konsistensi kedua pola grafik ditunjukkan juga oleh grafik waktu enkripsi dan dekripsi pada dokumen G-358.pdf, dimana pada titik dokumen tersebut mencapai puncak waktu eksekusi terutama pada metode *hybrid*. Hal tersebut memperkuat indikasi bahwa dokumen G-358.pdf memiliki karakteristik dokumen (ukuran dokumen dan isi dokumen) yang lebih kompleks dibandingkan dokumen yang lain. Dengan demikian, dapat disimpulkan bahwa performa antar algoritma selain dipengaruhi oleh karakteristik dokumen yang kompleks juga dipengaruhi oleh kompleksitas algoritma itu sendiri. AES yang memiliki struktur lebih efisien mampu mempertahankan performa terbaiknya, sementara *hybrid* mengalami peningkatan waktu eksekusi yang signifikan akibat proses enkripsi berlapis.

3.2. Analisis Entropi

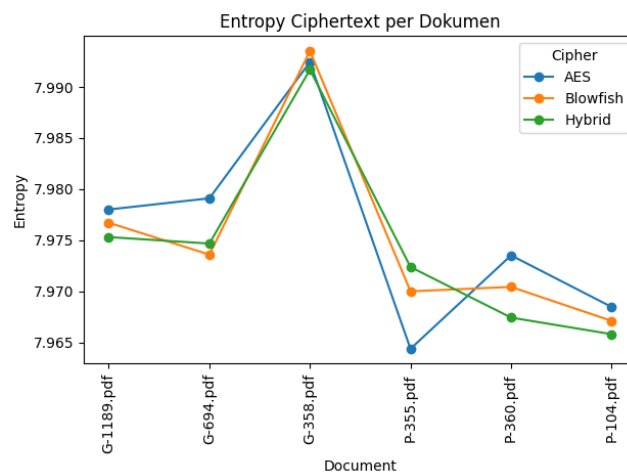
Berdasarkan hasil perhitungan rata-rata, ketiga pendekatan AES, *Blowfish* dan *hybrid* menunjukkan nilai entropi yang sangat tinggi dan relatif seragam, yakni berada pada kisaran 7,97. Nilai tersebut mendekati nilai maksimum entropi yaitu 8. Hal ini, mengindikasikan bahwa *ciphertext* yang dihasilkan

memiliki tingkat keacakan yang sangat baik dan sulit diprediksi. Secara umum, AES menghasilkan nilai entropi relatif sedikit lebih tinggi dibandingkan *Blowfish* dan *hybrid* sebagaimana pada Tabel 5, meskipun perbedaan tersebut tidak terlalu signifikan.

Tabel 5. Komparasi Rata-Rata Nilai Entropi

Algoritma	Entropi
AES	7.975986
<i>Blowfish</i>	7.975227
<i>Hybrid</i> (AES + <i>Blowfish</i>)	7.974548

Hasil ini diperkuat oleh grafik pada Gambar 7 yang menunjukkan bahwa distribusi nilai entropi pada seluruh dokumen cenderung stabil dan cenderung tidak mengalami fluktuasi yang besar. Pada grafik tersebut, AES, *Blowfish* dan *hybrid* memiliki pola yang hampir sejajar, menandakan bahwa kemampuan dalam menghasilkan keacakan *ciphertext* relatif setara. Puncak nilai terjadi pada dokumen G-358.pdf, dimana seluruh algoritma mencapai nilai mendekati 7,99. Hal ini menunjukkan bahwa dokumen tersebut pada proses enkripsi menghasilkan distribusi karakter yang paling acak dibandingkan dokumen lainnya.



Gambar 7. Hasil *Shannon entropy* tiap dokumen

Berbeda dengan dokumen P-355.pdf khususnya pada AES, yang nilai entropinya berada pada puncak terendah meskipun nilainya tetap berada pada kisaran tinggi. Hal ini mengindikasikan bahwa variasi karakteristik dokumen, seperti panjang teks atau distribusi karakter awal dapat mempengaruhi hasil entropi, namun tidak secara signifikan menurunkan kualitas keamanan.

3.3. Analisis *Avalanche Effect*

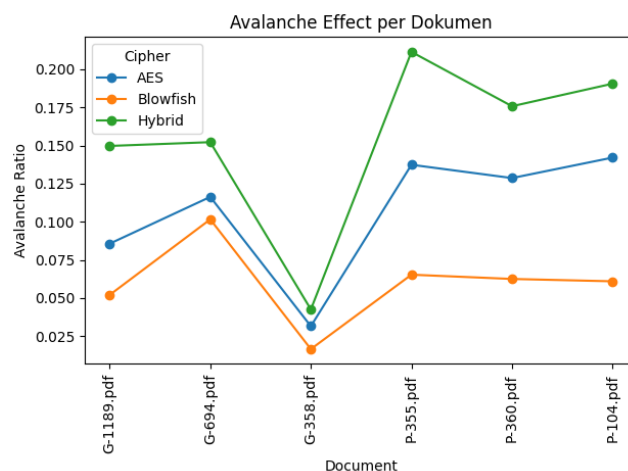
Hasil rata-rata dari perhitungan yang diperoleh sebagaimana pada Tabel 6, metode *hybrid* menghasilkan nilai *avalanche* tertinggi sebesar 0,154, diikuti oleh AES sebesar 0,107, dan *Blowfish* sebesar 0,060. Nilai ini menunjukkan bahwa *hybrid* memiliki kemampuan difusi yang paling baik, yaitu mampu menghasilkan perubahan *ciphertext* yang signifikan terhadap perubahan kecil pada *plaintext*.

Tabel 6. Komparasi Rata-Rata Nilai *Avalanche Effect*

Algoritma	<i>Avalanche</i>
AES	0.106908
<i>Blowfish</i>	0.059807
<i>Hybrid</i> (AES + <i>Blowfish</i>)	0.153652

Hasil ini diperkuat oleh grafik pada Gambar 8 yang menunjukkan pola konsisten di seluruh dokumen. Pada grafik, *hybrid* (garis hijau) secara dominan berada di posisi tertinggi dibandingkan AES (garis biru) dan *Blowfish* (garis oranye). Hal ini mengindikasikan bahwa kombinasi algoritma dalam

pendekatan *hybrid* mampu meningkatkan kompleksitas transformasi data sehingga menghasilkan *avalanche effect* yang lebih kuat.



Gambar 8. Grafik *avalanche* tiap dokumen

Secara rinci, nilai *avalanche* tertinggi terlihat pada dokumen P-355.pdf, dimana pada *hybrid* dokumen tersebut dapat mencapai nilai diatas 0,20, jauh lebih tinggi dibandingkan AES dan *Blowfish* pada dokumen yang sama. Sebaliknya, nilai *avalanche* terendah ada pada dokumen G-358.pdf, khususnya pada *Blowfish* yang berada dibawah 0,025. Penurunan ini juga terlihat pada AES dan *hybrid*, meskipun tetap mempertahankan nilai yang lebih tinggi dibandingkan *Blowfish*. Hal ini dapat dikatakan bahwa karakteristik dokumen seperti panjang teks dan kompleksitas isi dokumen dapat mempengaruhi tingkat difusi, meskipun tidak mengubah pola dominasi antar algoritma.

3.4. Pembahasan

Berdasarkan hasil analisis yang telah dilakukan, evaluasi terhadap parameter waktu eksekusi, entropi dan *avalanche effect* menunjukkan bahwa masing-masing algoritma memiliki karakteristik performa dan tingkat keamanan yang berbeda. Pada parameter waktu eksekusi, AES menunjukkan performa terbaik dengan waktu eksekusi paling cepat dibandingkan *Blowfish* dan *hybrid*. Hasil ini sejalan dengan penelitian yang dilakukan oleh [8] serta diperkuat oleh [16] yang menunjukkan bahwa performa AES lebih unggul dibandingkan *Blowfish*. Keunggulan tersebut dipengaruhi oleh struktur internal AES yang menggunakan ukuran blok tetap 128 bit serta proses transformasi yang terstandarisasi, sehingga enkripsi dan dekripsi dapat dilakukan secara lebih efisien. Sebaliknya, *Blowfish* menggunakan struktur *Feistel network* dan proses *key expansion* yang relatif lebih kompleks, sehingga membutuhkan waktu eksekusi yang lebih tinggi dibandingkan AES meskipun menggunakan panjang *key* yang sama pada penelitian ini.

Pada parameter entropi AES, *Blowfish* dan *hybrid* sama-sama menghasilkan nilai yang tinggi dan hampir mendekati nilai maksimum. Hal ini menunjukkan bahwa *ciphertext* yang dihasilkan memiliki tingkat keacakan dan ketidakpastian yang tinggi, sehingga sulit diprediksi. Semakin tinggi nilai entropi, maka semakin baik kualitas enkripsi dalam menghasilkan distribusi data yang acak dan menjaga kerahasiaan informasi. Temuan ini diperkuat oleh penelitian [9] yang menyatakan bahwa AES dan *Blowfish* memiliki tingkat keamanan tinggi karena didukung oleh panjang kunci yang besar serta desain algoritma yang efektif dalam menghasilkan *ciphertext* yang kompleks. Berbeda dengan parameter entropi, pada *avalanche effect* metode *hybrid* menghasilkan nilai tertinggi dibandingkan dengan AES dan *Blowfish*. Kondisi ini menunjukkan bahwa *hybrid* dengan enkripsi berlapisnya lebih optimal dalam memperkuat aspek difusi, di mana perubahan kecil pada *plaintext* dapat menghasilkan perubahan yang lebih luas pada *ciphertext*. Namun, peningkatan difusi tersebut tidak secara otomatis meningkatkan entropi, karena entropi lebih merepresentasikan tingkat keacakan global yang berkaitan dengan aspek *confusion*. Dengan demikian, *hybrid* lebih unggul dalam sensitivitas perubahan data, tetapi tidak menunjukkan perbedaan signifikan pada distribusi keacakan *ciphertext* karena AES dan *Blowfish* secara individual telah memiliki mekanisme *confusion* yang kuat.

Temuan ini menunjukkan bahwa pemilihan algoritma perlu disesuaikan dengan kebutuhan keamanan dan efisiensi. Dari sisi implikasi pada Pengadilan Agama, hasil ini menunjukkan adanya *trade-off* antara keamanan dan efisiensi. Metode *hybrid* lebih sesuai untuk dokumen yang bersifat sangat rahasia seperti dokumen permohonan dan gugatan yang mengandung data sensitif dari para pihak berperkara, karena memberikan tingkat keamanan lebih tinggi melalui *avalanche effect* yang lebih baik, meskipun membutuhkan biaya komputasi lebih besar. Sebaliknya, AES lebih cocok digunakan pada dokumen operasional karena lebih efisien dengan tingkat keamanan yang tetap memadai. Penelitian ini masih memiliki keterbatasan, yaitu jumlah dokumen yang terbatas, variasi ukuran data yang belum beragam, serta penggunaan satu *platform* eksperimen sehingga generalisasi hasil masih terbatas. Selain itu, belum terdapat perbandingan eksplisit dengan studi lain karena adanya perbedaan objek penelitian, karakteristik dataset, ukuran dokumen serta skema pengujian yang digunakan. Oleh karena itu, pembahasan komparatif dalam penelitian ini difokuskan pada karakteristik performa dan tingkat keamanan masing-masing algoritma.

4. KESIMPULAN

Berdasarkan hasil penelitian beserta pembahasan yang telah dilakukan, dapat disimpulkan bahwa algoritma AES, *Blowfish* dan metode *hybrid* memiliki karakteristik performa yang berbeda baik dari aspek kecepatan maupun keamanan. Dari aspek kecepatan (waktu eksekusi) AES terbukti menjadi algoritma paling efisien dengan rata-rata waktu enkripsi dan dekripsi tercepat dibandingkan algoritma lainnya. *Blowfish* pada posisi tengah sedangkan *hybrid* menduduki posisi terakhir dengan waktu eksekusi paling lama akibat penerapan enkripsi berlapis yang meningkatkan kompleksitas komputasi. Dari aspek keamanan, AES, *Blowfish* dan *hybrid* menunjukkan hasil entropi yang sangat tinggi dan mendekati nilai maksimum, yang menandakan bahwa seluruh metode mampu menghasilkan *ciphertext* dengan tingkat keacakan (*randomness*) yang baik. Namun demikian, parameter *avalanche* menunjukkan perbedaan yang lebih signifikan di mana metode *hybrid* memiliki nilai tertinggi, diikuti AES dan *Blowfish*. Hal ini menunjukkan bahwa metode *hybrid* memiliki kemampuan difusi yang lebih kuat, sehingga lebih tahan terhadap serangan kriptanalisis. Selain itu, hasil pengujian pada berbagai dokumen menunjukkan bahwa variasi karakteristik dokumen seperti ukuran dokumen, panjang teks dan kompleksitas isi juga dapat mempengaruhi waktu eksekusi dan nilai *avalanche* namun tidak mengubah pola perbandingan antar algoritma. AES secara konsisten unggul dalam kecepatan, sedangkan *hybrid* unggul dalam aspek keamanan.

Berdasarkan temuan tersebut, pemilihan metode enkripsi di lingkungan pengadilan agama sebaiknya disesuaikan dengan kebutuhan sistem. Untuk dokumen operasional yang memerlukan efisiensi tinggi, algoritma AES lebih direkomendasikan, sedangkan untuk dokumen yang sangat sensitif, metode *hybrid* dapat diimplementasikan guna meningkatkan keamanan melalui enkripsi berlapis. *Blowfish* dapat menjadi alternatif dengan performa yang relatif seimbang, meskipun tidak unggul secara signifikan pada kedua aspek tersebut. Secara teknis, disarankan penggunaan IV (*initialization vector*) yang acak dan unik pada setiap proses enkripsi, pengelolaan kunci yang aman, serta integrasi dengan sistem manajemen dokumen digital untuk memastikan perlindungan data secara menyeluruh. Sebagai arah penelitian selanjutnya, beberapa pengembangan dapat dilakukan untuk meningkatkan kualitas dan relevansi penelitian. Pertama, penggunaan metode operasi yang lebih modern dan aman seperti GCM (*Galois/ Counter Mode*) dapat dipertimbangkan untuk menyediakan fitur autentikasi selain kerahasiaan. Kedua, pengujian dapat diperluas pada skenario sistem nyata dengan *volume* data yang lebih besar dan lingkungan jaringan yang berbeda untuk memperoleh hasil yang lebih representatif. Ketiga, penelitian lanjutan dapat mengeksplorasi kombinasi algoritma lain atau pendekatan lain yang lebih efisien guna mengurangi *overhead* komputasi tanpa mengurangi tingkat keamanan. Selain itu, integrasi sistem berbasis *cloud* atau *e-government* juga dapat menjadi peluang penelitian yang menjanjikan.

5. DAFTAR PUSTAKA

- [1] Wasis, "Caesar Cipher Algorithm in Message Security," *Jurnal Inotera*, vol. 11, no. 1, hlm. 66–70, Feb 2026, doi: 10.31572/inotera.Vol11.Iss1.2026.ID578.

- [2] H. A. Sharath, J. Vrindavanam, S. Dana, dan S. N. Prasad, "Quantum-Resilient Cryptography: A Survey on Classical and Quantum Algorithms," *IEEE Access*, vol. 13, hlm. 172854–172877, 2025, doi: 10.1109/ACCESS.2025.3612982.
- [3] M. Habib Maulana, M. Tahir, N. Farroha, F. Maulana, dan R. Rurye Apriliyani, "Perancangan Sistem Keamanan File Menggunakan Hybrid Encryption untuk Perlindungan Data," *Jurnal Restikom : Riset Teknik Informatika dan Komputer*, vol. 7, no. 1, hlm. 87–96, 2025, [Daring]. Tersedia pada: <https://restikom.nusaputra.ac.id>
- [4] D. Ramakrishna dan M. Ali Shaik, "A Comprehensive Analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges," *IEEE Access*, vol. 13, hlm. 11576–11593, 2025, doi: 10.1109/ACCESS.2024.3518533.
- [5] A. P. Indraka dan M. A. Romli, "Keamanan Arsip Kelurahan Bumijo Menggunakan Metode Advanced Encryption Standard (AES 128) Berbasis Web," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 1, hlm. 232–241, Des 2024, doi: 10.57152/malcom.v5i1.1728.
- [6] D. E. Ramadhani, P. Nurul Sabrina, dan H. Ashaury, "Implementasi Algoritma Enkripsi Blowfish dan Rijndael dalam Pengamanan File Text," *Jurnal Locus: Penelitian & Pengabdian*, 2025, [Daring]. Tersedia pada: <https://locus.rivierapublishing.id/index.php/jl>
- [7] M. Zuna, A. Wulansari, dan A. B. Putra, "Perbandingan Algoritma Kriptografi Simetris dan Asimetris Dalam Keamanan Data Digital," *Jurnal Mahasiswa Teknik Informatika*, vol. 10, no. 1, 2026.
- [8] F. Dwi Insani dan M. Dwi Anggraeni, "Analisis Kinerja Algoritma Advanced Encryption Standard (AES) Encryption dan Algoritma Blowfish pada Proses Enkripsi dan Dekripsi," *Jurnal TRANSFORMASI*, vol. 21, no. 2, hlm. 147–156, 2025.
- [9] F. Rifaldy, H. P. Limbong, M. Firjatullah, R. A. Gading, I. Prayoga, dan I. Rusydi, "Perbandingan Algoritma DES, AES, IDEA, dan Blowfish Berdasarkan Panjang Kunci dan Ciphertext Sebagai Indikator Keamanan Data," *JORAPI : Journal of Research and Publication Innovation*, vol. 4, no. 1, 2026.
- [10] P. Daffa Dwiyanah, F. Fathurrohman, N. Alfikry, dan J. Sunupurwa Asri, "A Comparative Analysis of the Advanced Encryption Standard (AES) 128-, 192-, and 256-Bit Algorithms in Digital Data Security," *Jurnal Multidisiplin Sahombu*, vol. 6, no. 02, hlm. 176–182, 2026.
- [11] R. Sabilillah Saputra dkk., "Analisis Komparasi Performansi Algoritma Kriptografi RSA dan AES pada Keamanan Data Teks," 2026.
- [12] N. Muzakki dan N. Rochmah Dyah Puji Astuti, "Optimasi Kunci Kriptografi XOR menggunakan Metode Hibrida Algoritma Genetika dan Simulated Annealing Optimization of XOR Cryptographic Keys using a Hybrid Genetic Algorithm and Simulated Annealing," *Sistemasi: Jurnal Sistem Informasi*, 2026, [Daring]. Tersedia pada: <http://sistemasi.ftik.unisi.ac.id>
- [13] M. N. Z. Soleh, "Kriptografi Homomorfik dalam Anonimisasi Data untuk Pengolahan Data pada Sistem E-Voting," *Jurnal Masyarakat Informatika*, vol. 15, no. 2, hlm. 107–124, Nov 2024, doi: 10.14710/jmasif.15.2.66317.
- [14] K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, dan S. Ariffin, "Analyse on Avalanche Effect in Cryptography Algorithm," dalam *Proceedings of the International Conference on Sustainable Practices, Development and Urbanisation (IConsPADU 2021), 16 November 2021, Universiti Selangor (UNISEL), Malaysia*, European Publisher, Okt 2022, hlm. 610–618. doi: 10.15405/epms.2022.10.57.
- [15] M. Adharis Adlani dan R. E. Putra, "Pengamanan Mnemonic Phrase Menggunakan Modified Advanced Encryption Standart," *Journal of Informatics and Computer Science*, vol. 03, 2022.
- [16] R. Fadlan Fahira Siregar, N. Dly, S. Wulandari, P. Kurni Wati, N. Agustina Siregar, dan I. Rusydi, "Comparative Analysis of Encryption and Decryption Speed of AES and Blowfish Algorithms on Various File Size," *IJGAM: Interdisciplinary Journal of Global and Multidisciplinary*, vol. 2, no. 1, 2026.