Skema Pendanaan: Madya

LAPORAN PENELITIAN

Analisis Perbandingan Kinerja Algoritma Camellia dan AES

PENELITI

Teja Endra Eng Tju, S.T., M.Kom. (190046)

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS BUDI LUHUR

Agustus 2025

HALAMAN PENGESAHAN
LAPORAN PENELITIAN

Judul Penelitian : Analisis Perbandingan Kinerja Algoritma Camellia dan AES

Bidang Penelitian : ICT

Ketua Peneliti

a. Nama Lengkap : Teja Endra Eng Tju, S.T., M.Kom.
b. NIP/NIDN/ID-SINTA : 190046/0407127201/6713276
c. Jabatan Fungsional : Lektor
d. Program Studi : Sistem Informasi
e. Nomor HP : +628998909707
f. Alamat e-mail : teja.endraengtju@budiluhur.ac.id

Anggota Peneliti

a. Nama Lengkap : -
b. NIP/NIDN/ID-SINTA : -

Mahasiswa (1)

a. Nama Lengkap : Fauzi Alfadhillah
b. NIM : 2311501767

Mahasiswa (2)

a. Nama Lengkap : -
b. NIM : -

Lama Penelitian : 6 bulan

Biaya Penelitian

a. Sumber Universitas Budi Luhur : Rp. 7.500.000,00
b. Sumber lain (sebutkan jika ada) : Rp. -

Jakarta, 01 Agustus 2025

Mengetahui,
Dekan Fakultas Teknologi Informasi

(Dr. Ir. Achmad Solichin, S.Kom., M.T.I.)
NIP 190025

Ketua Pelaksana

(Teja Endra Eng Tju, S.T., M.Kom.)
NIP 190046

Menyetujui,
Direktur Riset dan Pengabdian Kepada Masyarakat

(Prof. Dr. Ir. Prudensius Maring, M.A.)
NIP 190043

No. Registrasi : 0 1 5 0 1 LPJ 0 7 2 5
Tanggal : 3 1 0 7 2 5 Paraf :

RINGKASAN

Urgensi penelitian ini untuk mengantisipasi risiko siber yang semakin canggih, seperti *ransomware* dan serangan berbasis kecerdasan artifisial, mengancam integritas data sensitif. Dalam menghadapi tantangan ini, pemilihan algoritma kriptografi yang tepat sangat penting untuk melindungi data dan menjaga efektivitas operasional sistem.

Tujuan penelitian ini adalah untuk membandingkan kinerja algoritma kriptografi Camellia dan AES, baik dari segi efisiensi selama proses enkripsi dan dekripsi, serta aspek keamanan kedua algoritma terhadap serangan kriptografi. Hasil penelitian ini diharapkan dapat memberikan panduan dalam memilih algoritma yang paling sesuai untuk aplikasi yang membutuhkan perlindungan data yang kuat.

Metode yang digunakan dalam penelitian ini adalah eksperimen dengan mengenkripsi 72 *file* yang bervariasi dalam ukuran dan format (*.mp3, *.jpg, *.png, *.pdf, *.docx, *.xls, *.pptx, dan *.txt), dengan setiap jenis *file* diuji pada 3 ukuran acuan berbeda, dan setiap ukuran terdiri dari 3 *file*. Kedua algoritma, yaitu Camellia dan AES, diterapkan dengan panjang kunci 256-bit untuk memastikan tingkat keamanan yang tinggi selama proses enkripsi dan dekripsi. Efisiensi algoritma dalam proses enkripsi dan dekripsi diukur dengan mencatat waktu eksekusi, konsumsi memori, penggunaan prosesor, dan ukuran *file* terenkripsi. Aspek keamanan kriptografi dievaluasi melalui simulasi serangan terhadap *file* terenkripsi dengan teknik *Dictionary Attack, Birthday Attack*, dan *Brute-force Attack*.

Luaran penelitian ini memberikan pemahaman tentang perbandingan kinerja algoritma enkripsi dan relevansinya dalam menghadapi ancaman siber saat ini. Selain itu, hasil eksperimen diharapkan berkontribusi pada pemilihan algoritma kriptografi yang optimal untuk pengamanan data di berbagai sektor. Target luaran wajib adalah sertifikat HKI dan pengajuan publikasi pada Jurnal Teknik Informatika dan Sistem Informasi terakreditasi Sinta 3.

Kata Kunci: Efisiensi Kriptografi; Enkripsi Data; Kriptanalisis; Keamanan Algoritma; Kinerja Enkripsi.

PRAKATA

Puji syukur ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga penelitian yang berjudul "Analisis Perbandingan Kinerja Algoritma Camellia dan AES" ini dapat diselesaikan dengan baik. Penelitian ini dilatarbelakangi oleh meningkatnya perhatian terhadap keamanan data, seiring dengan pesatnya perkembangan teknologi informasi yang menghubungkan berbagai sistem secara global. Penggunaan algoritma kriptografi menjadi metode utama dalam menjaga kerahasiaan dan integritas informasi digital.

Dari sekian banyak algoritma yang tersedia, Camellia dan AES (Advanced Encryption Standard) merupakan dua algoritma yang paling menonjol, dengan tingkat keamanan yang tinggi dan karakteristik yang berbeda. Camellia, dikembangkan oleh NTT dan Mitsubishi Electric, dikenal karena fleksibilitas dan efisiensinya dalam berbagai platform. Sementara itu, AES yang dikembangkan oleh NIST telah diakui luas sebagai standar enkripsi yang sederhana namun sangat kuat dan efisien. Kedua algoritma ini memiliki keunggulan tersendiri: Camellia menawarkan struktur yang fleksibel, sedangkan AES lebih diterima luas karena kesederhanaan dan efektivitasnya.

Penelitian ini bertujuan untuk menganalisis dan membandingkan kinerja kedua algoritma tersebut dalam proses enkripsi dan dekripsi terhadap berbagai jenis dan ukuran file. Selain aspek efisiensi, penelitian ini juga mengkaji ketahanan masing-masing algoritma terhadap potensi serangan kriptografi, guna memahami keunggulan dan keterbatasannya dalam menjaga keamanan data digital. Melalui pendekatan ini, diharapkan hasil penelitian dapat memberikan wawasan yang bermanfaat bagi pengembang dan praktisi dalam memilih algoritma kriptografi yang paling sesuai dengan kebutuhan spesifik dari sisi efisiensi maupun keamanan sistem.

Penulis menyadari bahwa keberhasilan penelitian ini tidak lepas dari dukungan berbagai pihak. Ucapan terima kasih disampaikan kepada Universitas Budi Luhur atas dukungan fasilitas, pembimbingan, dan pendanaan yang diberikan. Terima kasih juga kepada seluruh pihak sekolah yang telah berkontribusi dalam proses pengumpulan kebutuhan, pengujian, dan validasi sistem. Masukan yang diberikan sangat membantu dalam menyempurnakan penelitian ini.

Akhir kata, penulis menyadari bahwa masih terdapat kekurangan dalam pelaksanaan penelitian ini. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan guna penyempurnaan di masa yang akan datang.

Jakarta, 01 Agustus 2025

Peneliti

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I. PENDAHULUAN

1. Latar Belakang dan Rumusan Permasalahan

Keamanan data menjadi perhatian utama seiring berkembangnya teknologi informasi yang menghubungkan berbagai sistem global. Penggunaan algoritma kriptografi untuk melindungi data sensitif adalah cara utama untuk menjaga kerahasiaan dan integritas informasi [1]. Di antara berbagai algoritma kriptografi yang tersedia, Camellia [2] dan AES (*Advanced Encryption Standard*) [3] memiliki tingkat keamanan cukup tinggi dengan karakteristik berbeda. Camellia, yang dikembangkan oleh NTT (Nippon *Telegraph and Telephone*) dan Mitsubishi Electric, menawarkan struktur yang fleksibel dan efisien, serta dapat diterapkan pada berbagai platform [4]. Di sisi lain, AES, yang dikembangkan oleh NIST (National Institute of Standards and Technology), dikenal sebagai standar enkripsi yang sederhana namun sangat kuat dan efisien. Kedua algoritma ini unggul dalam hal keamanan, meskipun dengan pendekatan yang berbeda. Camellia lebih fleksibel, sementara AES lebih diterima karena kesederhanaan dan efektivitasnya.

Rumusan masalah dalam penelitian ini mencakup analisis kinerja algoritma Camellia dan AES dalam enkripsi dan dekripsi berbagai jenis dan ukuran data. Penelitian ini juga mengkaji alasan pemilihan kedua algoritma ini yang memiliki karakteristik dan keunggulan berbeda, serta mengidentifikasi sejauh mana efisiensi enkripsi dan dekripsi kedua algoritma memengaruhi performa sistem. Selain itu, penelitian ini mengidentifikasi perbedaan tingkat ketahanan Camellia dan AES terhadap berbagai jenis serangan kriptografi untuk memahami keunggulan dan keterbatasan masing-masing algoritma dalam menjaga keamanan data digital. Tujuan penelitian ini adalah untuk menganalisis perbedaan keduanya dalam efisiensi enkripsi, dekripsi, dan ketahanan terhadap serangan. Perbandingan kedua algoritma ini diharapkan memberikan wawasan tentang efektivitas dan ketahanan masing-masing, sehingga membantu dalam memilih algoritma yang paling sesuai dengan kebutuhan keamanan dan efisiensi. Hasil penelitian ini diharapkan menjadi panduan dalam memilih algoritma yang tahan terhadap ancaman yang berkembang.

2. Pendekatan Pemecahan Masalah

Pendekatan pemecahan masalah dalam penelitian ini dilakukan dengan mengenkripsi dan mendekripsi berbagai ukuran dan tipe *file,* yaitu teks, gambar, dan multimedia, yang diambil atau dibuat secara acak. Untuk membandingkan efisiensi kinerja algoritma Camellia dan AES dalam proses enkripsi dan dekripsi, dilakukan pencatatan waktu eksekusi, konsumsi memori, dan penggunaan prosesor, serta ukuran *file* terenkripsi. Dari sisi keamanan, penelitian ini akan melakukan simulasi serangan terhadap *file* terenkripsi, yaitu *Dictionary Attack* [5–9], *Birthday Attack* [10,11], dan *Brute-force* [12–18]. Hasil pengujian akan dianalisis untuk mengidentifikasi kelemahan dan kekuatan masing-masing algoritma dalam menjaga kerahasiaan dan integritas data. Dengan membandingkan efisiensi dan keamanan keduanya, penelitian ini bertujuan memberikan wawasan mengenai algoritma yang lebih sesuai untuk kebutuhan perlindungan data.

3. *State of The Art* dan Kebaruan

Penelitian mengenai algoritma kriptografi Camellia dan AES telah banyak dilakukan, terutama

terkait keamanan data dan ketahanan terhadap serangan kriptografi. AES telah menjadi standar internasional karena kemampuannya memberikan enkripsi kuat dan diterima luas dalam berbagai aplikasi keamanan [19]. Camellia menawarkan tingkat keamanan setara dengan AES, dengan struktur yang lebih fleksibel dan modular, memudahkan implementasi di berbagai platform dan skenario [20].

Penelitian sebelumnya terkait penerapan algoritma Camellia digunakan untuk *Authentication Encryption* pada *Wireless Robotics* [21] dan *Mobile Platforms* [22]; *Quantum Implementation* dengan S-box [23]; *Security Encryption* pada *e-Bank* [24] dan IoT [25]. Adapun terkait penerapan algoritma AES digunakan untuk Enkripsi Citra Digital termodifikasi [26]; Pengamanan Data untuk Rekam Medis [27], Transaksi [28], Gambar [29], Cloud Computing [30] dan Penjualan Sepatu [31]; Database Aplikasi [32], QR Code [33] dan Aplikasi *Chat* [34,35]; *Wireless Network* pada *Healthcare* [36]. Sedangkan terkait perbandingan kedua algoritma Camellia dan AES digunakan untuk *Quantum Implementation* dengan S-box [37]; Enkripsi Citra Digital dengan Uji NPCR dan UACI [38]; *Security Encryption* pada IoT [39]; *Transport 5G Network* dengan *Quantum Secured* [40]; *Authentication Encryption* untuk *Bus Network* [41]; *Security Cryptography* pada IoT [42] dan IoHT [43]; *Proxy Session Internet Protocol* [44]; Implementasi *Block Cipher* pada *framework* SAFARI [45] dan MISTY1[46].

Kebaruan penelitian ini terletak pada pendekatan evaluatif berupa eksperimen dan simulasi dalam mengukur efisiensi algoritma berdasarkan waktu, memori, dan penggunaan prosesor selama proses enkripsi dan dekripsi, serta mengevaluasi aspek keamanannya dalam menghadapi ancaman siber terhadap algoritma Camellia dan AES, terutama dalam konteks serangan siber yang berkembang seperti ransomware dan serangan berbasis kecerdasan artifisial. Penekanan utama pada penelitian ini adalah perbandingan kinerja dan ketahanan kedua algoritma terhadap serangan kriptografi dengan teknik *Dictionary Attack*, *Birthday Attack*, dan *Brute-force Attack*, yang belum banyak dibahas secara komprehensif pada penerapan dalam pengamanan data berukuran kecil hingga menengah. Urgensi dalam penelitian ini terkait dengan peningkatan ancaman siber yang semakin kompleks, seperti *ransomware* dan serangan berbasis kecerdasan artifisial, yang mengancam integritas data sensitif. Oleh karena itu, pemilihan algoritma kriptografi yang tepat sangat penting untuk melindungi data dan menjaga kinerja sistem.

4. Peta Jalan Penelitian

Roadmap lima tahun berfokus pada pengembangan keamanan siber, yang bertujuan untuk meningkatkan proteksi dan integritas sistem informasi di berbagai sektor. Gambar 1 menyajikan gambaran tentang kegiatan yang dijadwalkan setiap tahun.

Penelitian tahun pertama berjudul Evaluasi Keamanan Siber pada Portal Akademik Mahasiswa dengan Metode OWASP telah dilakukan dengan pengujian keamanan melalui *penetration testing* pada situs akademik untuk mengidentifikasi kerentanan. Temuan dari pengujian ini digunakan untuk memperbaiki kelemahan dan memberikan rekomendasi perbaikan. Penelitian ini telah diajukan publikasi ke jurnal CoreIT Sinta 3.

Tahun kedua, yaitu penelitian ini, fokus pada evaluasi dan analisis perbandingan kinerja antara algoritma kriptografi Camellia dan AES. Peneliti akan membandingkan performa, keamanan, dan efektivitas kedua algoritma dalam berbagai skenario data. Hasil penelitian ini diharapkan

dapat mengidentifikasi algoritma yang lebih efisien dan aman untuk diterapkan dalam sistem keamanan data.

Gambar 1. Diagram *Roadmap* Pengembangan Keamanan Siber Lima Tahun

Pada tahun ketiga, penelitian akan berfokus pada keamanan jaringan dengan machine learning. Peneliti akan menganalisis teknik *packet sniffing* untuk menyadap komunikasi jaringan dan dampaknya terhadap keamanan. Selain itu, akan dikembangkan mekanisme deteksi dan mitigasi serangan berbasis *machine learning* untuk meningkatkan perlindungan data dalam jaringan.

Tahun keempat berfokus pada keamanan aplikasi mobile. Penelitian akan menguji ketahanan aplikasi mobile terhadap serangan seperti *reverse engineering* dan *malware injection*. Selain itu, teknik proteksi seperti *code obfuscation* dan *runtime application self-protection* (RASP) akan diterapkan untuk meningkatkan keamanan aplikasi dari ancaman siber.

Pada tahun kelima, penelitian akan fokus pada pengembangan algoritma deteksi anomali. Peneliti akan merancang dan menguji algoritma untuk mendeteksi serangan siber dengan mengidentifikasi pola anomali dalam data. Evaluasi performa algoritma dilakukan untuk memastikan efektivitas sistem deteksi dalam mengenali ancaman siber secara akurat.

BAB II. METODE

Penelitian ini menggunakan pendekatan eksperimental untuk mengevaluasi kinerja algoritma Camellia dan AES berdasarkan tahapan yang ditunjukkan pada Gambar 2. Tahapan yang dilakukan mencakup Pengumpulan Data atau *File* yang terdiri dari berbagai jenis *file* serta Enkripsi dan Dekripsi *File* dengan Camellia dan AES. Uji Serangan Terhadap *File* Terenkripsi dilakukan untuk menguji ketahanan terhadap berbagai jenis serangan kriptografi. Selanjutnya, Analisis Kinerja Camellia dan AES membandingkan kecepatan, efisiensi, dan ketahanan kedua algoritma. Proses ini diakhiri dengan Evaluasi dan Kesimpulan untuk memberikan wawasan penggunaan algoritma yang lebih sesuai dalam konteks perlindungan data.

Gambar 2. Tahapan Metode Penelitian

Penelitian ini diawali dengan tahap pengumpulan data berupa 72 file yang terdiri dari sepuluh jenis file dengan format *.mp3, *.jpg, *.png, *.pdf, *.docx, *.xls, *.pptx, dan *.txt. Pemilihan format yang beragam bertujuan untuk mengevaluasi bagaimana algoritma Camellia dan AES menangani data dengan struktur yang berbeda, baik dari segi ukuran, kompleksitas, dan jenis informasinya. Data dikumpulkan secara acak dari berbagai sumber relevan, dengan setiap jenis file memiliki tiga ukuran berbeda, yaitu 100 KB, 1 MB, dan 10 MB. Ukuran tersebut diterapkan pada format file audio (.mp3), gambar (.jpg, .png), dokumen (.pdf, .docx, .xls, .pptx), dan plainteks (.txt). Tabel 1 menunjukkan distribusi file berdasarkan jenis dan ukuran.

Tabel 1. Distribusi Data

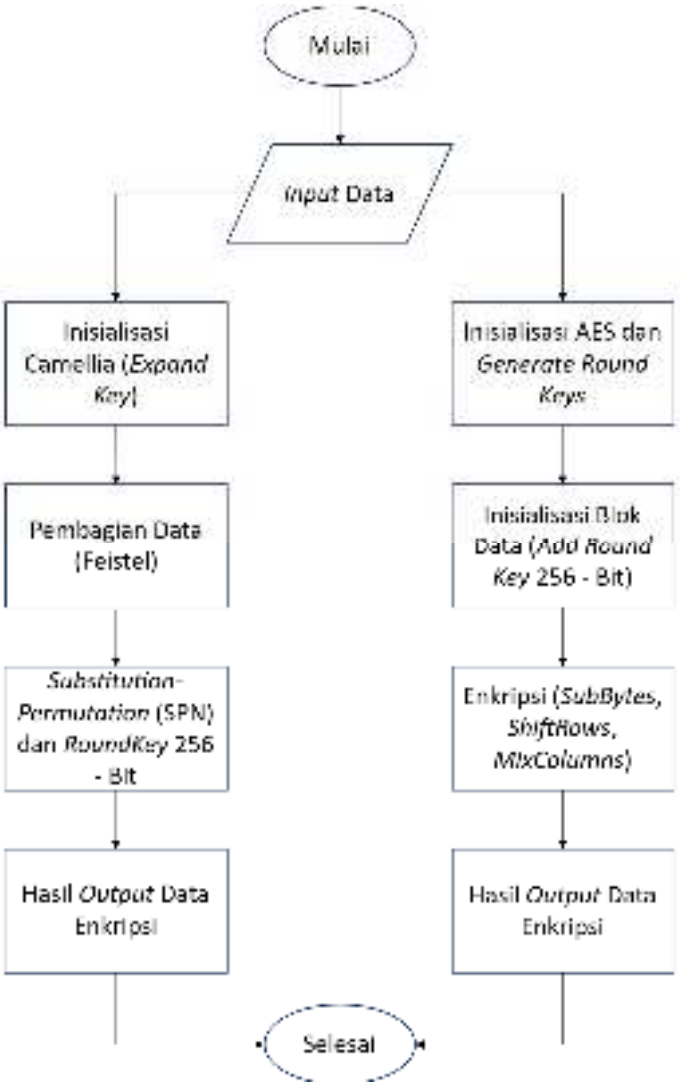
Tipe	Jumlah per Acuan Ukuran			Total
	100 KB	1 MB	10 MB	
*.mp3	3	3	3	9
*.jpg	3	3	3	9
*.png	3	3	3	9
*.pdf	3	3	3	9
*.docx	3	3	3	9
*.xls	3	3	3	9
*.pptx	3	3	3	9
*.txt	3	3	3	9
			Total Data	**72**

Setelah data terkumpul, penelitian memasuki tahap **Enkripsi dan Dekripsi *File* dengan Camellia dan AES.** Pengujian enkripsi, dekripsi, dan simulasi serangan dilaksanakan menggunakan laptop berprosesor AMD Ryzen 7 5800H, RAM 16GB, GPU NVIDIA GeForce RTX 3050 Ti, dengan sistem operasi Windows 11**.** *File* data yang telah disiapkan akan dienkripsi dan didekripsi dengan menggunakan panjang kunci 256-bit, yang diterapkan sesuai dengan masing-masing algoritma [47,48]. Pemilihan panjang kunci 256-bit didasarkan pada pemenuhan standar keamanan modern dan dapat menangani berbagai jenis serangan kriptanalisis. Kata sandi yang kuat digunakan untuk menghasilkan setiap kunci enkripsi [49]. Proses enkripsi dan dekripsi ini dilakukan menggunakan aplikasi berbasis *web* sederhana yang dikembangkan dengan *library* PyCryptodome [50,51] yang mencatat waktu eksekusi, penggunaan CPU, dan penggunaan RAM. Prosedur ini memungkinkan pengamatan terhadap bagaimana setiap algoritma menangani berbagai jenis file dan beban kerja, serta menyoroti perbedaan dalam efisiensi dan konsistensi pemrosesan. Gambar 3 menunjukkan diagram alir enkripsi dan dekripsi dengan algoritma Camellia dan AES 256-bit yang menggambarkan tahapan proses tersebut.

Tahap berikutnya adalah **Uji Serangan Terhadap *File* Terenkripsi** untuk menguji ketahanan masing-masing terhadap berbagai ancaman kriptografi. Dalam tahap ini, beberapa jenis serangan akan disimulasikan, termasuk *Dictionary Attack*, *Birthday Attack*, dan *Brute-Force Attack*. Simulasi ini bertujuan untuk mengidentifikasi potensi kelemahan dari kedua algoritma serta, mengetahui sejauh mana masing-masing mampu bertahan terhadap upaya pembobolan. Secara khusus, penelitian akan mengevaluasi apakah ada pola tertentu dalam proses enkripsi yang dapat dimanfaatkan oleh penyerang untuk mempercepat proses dekripsi tanpa kunci yang sah. Dengan melakukan simulasi serangan, penelitian ini tidak hanya menilai keamanan algoritma secara teoretis, tetapi juga menguji ketahanannya dalam skenario nyata berdasarkan *file* yang telah dienkripsi. Hasil pengujian ini akan memberikan wawasan mengenai keandalan kedua algoritma dalam menghadapi ancaman kriptografi yang semakin berkembang.

Setelah tahap enkripsi dan serangan, langkah selanjutnya adalah **Analisis Kinerja Camellia dan AES** berdasarkan hasil enkripsi dan dekripsi. Pada tahap ini, penelitian ini akan mengukur waktu yang dibutuhkan oleh algoritma Camellia dan AES untuk mengenkripsi serta mendekripsi berbagai jenis *file*. Selain mengukur kecepatan pemrosesan, ukuran *file* hasil enkripsi juga akan dibandingkan untuk menilai apakah terdapat perubahan signifikan yang dapat mempengaruhi efisiensi penyimpanan. Selanjutnya, penelitian ini akan mengevaluasi kecocokan masing-masing algoritma terhadap jenis data tertentu berdasarkan hasil yang

diperoleh. Parameter yang digunakan untuk perbandingan mencakup waktu yang dibutuhkan untuk enkripsi dan dekripsi, ukuran *file* hasil enkripsi, serta efisiensi penggunaan sumber daya sistem. Hasil analisis ini diharapkan dapat memberikan gambaran komprehensif mengenai efisiensi kedua algoritma dalam menangani berbagai jenis data.



Gambar 3. Alur Tahapan Enkripsi Algoritma Camellia dan AES

Tahap terakhir adalah **Evaluasi dan Kesimpulan** berdasarkan seluruh hasil yang telah diperoleh. Pada tahap ini, penelitian akan merangkum keunggulan dan kelemahan masing-masing algoritma dalam hal efisiensi dan keamanan. Hasil evaluasi akan digunakan untuk memberikan rekomendasi terkait algoritma yang lebih sesuai digunakan dalam konteks perlindungan data perusahaan. Kesimpulan ini diharapkan dapat menjadi dasar bagi pengambil keputusan dalam memilih algoritma kriptografi yang optimal sesuai dengan kebutuhan keamanan dan performa sistem yang diinginkan. Hasil eksperimen ini diharapkan dapat memberikan kontribusi dalam pemilihan algoritma kriptografi yang lebih tepat dan optimal untuk pengamanan data di berbagai sektor, seperti sektor perbankan, kesehatan, dan pemerintahan, yang sangat bergantung pada perlindungan data sensitif.

BAB III. HASIL PELAKSANAAN PENELITIAN

Hasil pengumpulan data mencakup 72 file dari delapan jenis file dengan tiga kategori ukuran yang telah acukan. Tabel 2 menyajikan tiga sampel file untuk setiap kategori ukuran yang telah acukan, diberi label File 1, File 2, dan File 3, dengan ukuran aktual bervariasi dalam rentang toleransi ±5%. Penggunaan tiga file per kategori ukuran memiliki beberapa tujuan. Hal ini memastikan hasil yang konsisten dan andal dalam setiap kelompok ukuran, menangkap variasi kecil dalam struktur dan konten file yang dapat memengaruhi pemrosesan, serta membantu mengurangi potensi bias akibat ketergantungan pada satu file saja.

Tabel 2. Distribusi Variasi File

Tipe *File*	**Ukuran Acuan**	**Ukuran Asli**		
		File 1	**File 2**	**File 3**
*.mp3	100 KB	1.02 KB	1.03 KB	1.02 KB
	1 MB	1.00 MB	1.04 MB	1.00 MB
	10 MB	10.03 MB	10.03 MB	10.04 MB
*.jpg	100 KB	1.05 KB	1.00 KB	1.00 KB
	1 MB	1.05 MB	1.05 MB	1.00 MB
	10 MB	10.03 MB	10.01 MB	10.02 MB
*.png	100 KB	1.01 KB	1.01 KB	1.01 KB
	1 MB	1.01 MB	1.00 MB	1.01 MB
	10 MB	10.02 MB	10.02 MB	10.04 MB
*.pdf	100 KB	1.00 KB	1.00 KB	1.01 KB
	1 MB	1.04 MB	1.05 MB	1.00 MB
	10 MB	10.00 MB	10.01 MB	10.01 MB
*.docx	100 KB	1.00 KB	1.04 KB	1.05 KB
	1 MB	1.02 MB	1.01 MB	1.01 MB
	10 MB	10.01 MB	10.05 MB	10.04 MB
*.xls	100 KB	1.00 KB	1.04 KB	1.00 KB
	1 MB	1.00 MB	1.01 MB	1.01 MB
	10 MB	10.04 MB	10.02 MB	10.01 MB
*.pptx	100 KB	1.04 KB	1.05 KB	1.00 KB
	1 MB	1.00 MB	1.05 MB	1.05 MB
	10 MB	10.04 MB	10.04 MB	10.04 MB
*.txt	100 KB	1.01 KB	1.03 KB	1.00 KB
	1 MB	1.01 MB	1.00 MB	1.01 MB
	10 MB	10.05 MB	10.05 MB	10.02 MB

Efisiensi enkripsi dan dekripsi dari algoritma Camellia dan AES dievaluasi menggunakan tiga metrik yaitu, Waktu Proses (*Run Time*), Penggunaan CPU, dan Konsumsi RAM. Waktu Proses merujuk pada waktu yang dibutuhkan untuk menyelesaikan proses enkripsi atau dekripsi, Penggunaan CPU menunjukkan persentase sumber daya prosesor yang digunakan selama eksekusi, dan Konsumsi RAM mencerminkan jumlah memori yang digunakan selama operasi berlangsung.

Untuk memastikan perbandingan yang representatif, nilai dari setiap metrik dirata-ratakan per jenis file menggunakan data dari tiga file dalam setiap kategori ukuran yang telah ditentukan sebelumnya, karena hasil evaluasi dari File 1, File 2, dan File 3 menunjukkan nilai yang konsisten dan mengindikasikan kinerja yang stabil. Pengukuran antar format dan ukuran file

juga relatif seragam dalam setiap kelompok, tanpa penyimpangan signifikan, yang mendukung validitas dari nilai rata-rata tersebut.

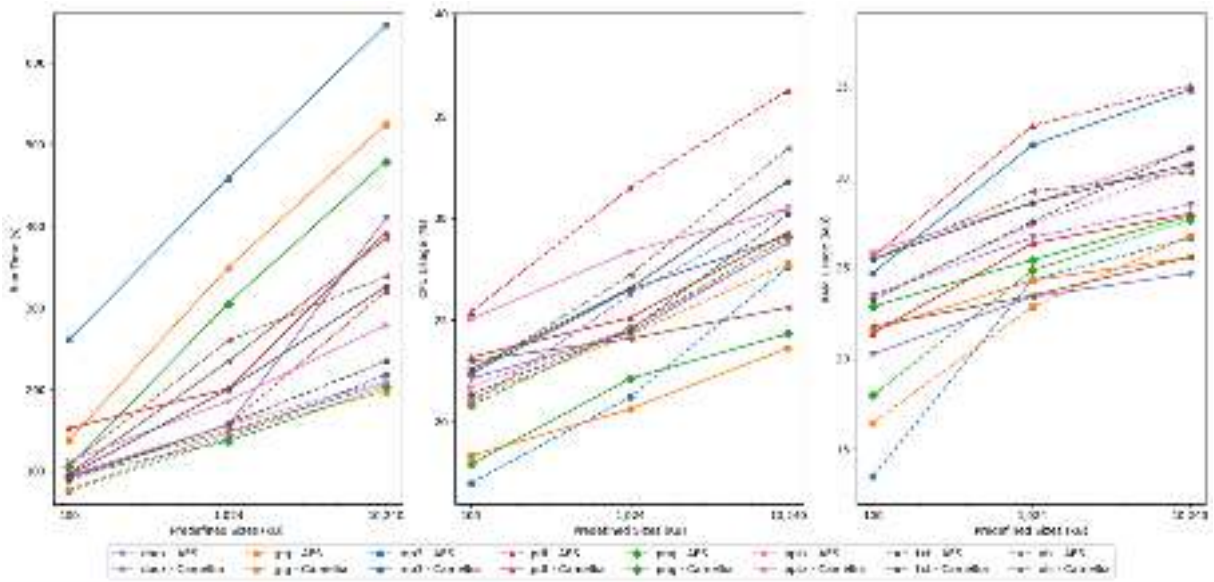
Hasil enkripsi disajikan dalam Tabel 3, yang menunjukkan rata-rata Waktu Proses, Penggunaan CPU, dan Konsumsi RAM untuk setiap jenis file dan ukuran yang telah ditentukan. Untuk menjaga konsistensi satuan dan menyederhanakan perbandingan numerik, ukuran file didefinisikan sebagai 100 KB, 1024 KB, dan 10240 KB, bukan menggunakan satuan campuran seperti 1MB dan 10MB. Metrik-metrik ini menggambarkan bagaimana kinerja masing-masing algoritma merespons peningkatan ukuran file, sehingga memberikan gambaran yang lebih jelas tentang efisiensi dan penggunaan sumber daya selama proses enkripsi.

Tabel 3. Ringkasan Rata-rata Proses Enkripsi

Tipe *File*	**Ukuran Acuan**	**Waktu Proses *(s)***		***CPU Usage (%)***		***RAM Usage (MB)***	
		Camellia	**AES**	**Camellia**	**AES**	**Camellia**	**AES**
*.mp3	100 KB	260.61	75.83	22.37	17.00	24.72	13.49
	1024 KB	458.64	140.65	28.49	21.22	31.76	24.33
	10240 KB	646.16	217.75	32.11	27.59	34.81	26.66
*.jpg	100 KB	137.59	77.30	18.34	21.12	21.54	16.46
	1024 KB	349.24	147.29	20.64	24.28	24.30	22.83
	10240 KB	524.70	197.32	23.62	27.75	25.57	26.77
*.png	100 KB	104.53	93.44	17.93	20.80	22.87	17.96
	1024 KB	305.27	136.36	22.13	24.59	25.43	24.85
	10240 KB	479.15	203.79	24.32	29.04	27.87	27.64
*.pdf	100 KB	152.16	192.21	23.17	25.39	21.39	25.61
	1024 KB	200.60	256.51	25.11	31.47	26.35	32.83
	10240 KB	392.14	340.52	29.29	36.25	27.99	35.03
*.docx	100 KB	91.98	94.97	22.13	20.88	20.25	23.51
	1024 KB	156.01	149.13	24.37	26.25	23.41	26.67
	10240 KB	409.58	206.79	28.81	30.49	24.68	28.47
*.xls	100 KB	96.38	107.52	22.99	22.37	21.78	25.47
	1024 KB	234.36	259.62	24.08	27.21	23.46	29.20
	10240 KB	384.74	338.61	25.61	33.40	25.59	30.26
*.pptx	100 KB	111.67	95.38	25.04	21.73	25.88	23.38
	1024 KB	185.69	156.13	28.36	24.59	28.55	27.39
	10240 KB	278.82	209.68	30.46	28.76	31.51	30.61
*.txt	100 KB	94.74	88.50	22.57	21.35	25.46	23.23
	1024 KB	199.99	157.52	26.55	24.50	28.58	27.54
	10240 KB	325.68	234.29	31.80	30.16	30.72	31.59

Berdasarkan Tabel 3, Gambar 4 memvisualisasikan proses enkripsi menggunakan skala logaritmik pada sumbu x untuk menunjukkan ukuran file (100 KB, 1024 KB, dan 10240 KB), memungkinkan analisis tren efisiensi yang lebih akurat. Grafik tersebut menunjukkan bahwa semakin besar ukuran file, semakin tinggi waktu proses, penggunaan CPU, dan konsumsi RAM, dengan efisiensi algoritma yang berbeda-beda tergantung pada jenis file.

Sejalan dengan proses enkripsi, metrik dekripsi untuk Waktu Proses, Penggunaan CPU, dan Konsumsi RAM dicatat dan dirata-ratakan berdasarkan ukuran file yang telah ditentukan, sebagaimana ditunjukkan dalam Tabel 4.

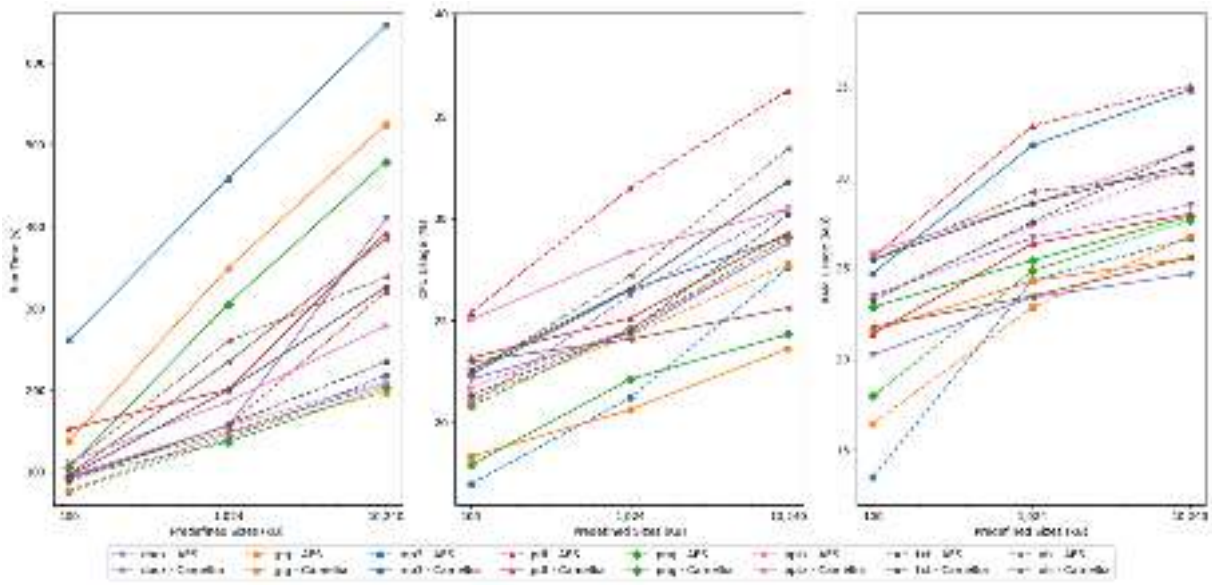


Gambar 4. Visualisasi Parameter Enkripsi

Tabel 4 menjadi dasar pada Gambar 5 yang menggambarkan efisiensi dekripsi dari algoritma Camellia dan AES. Sama halnya dengan proses enkripsi, peningkatan ukuran file umumnya menyebabkan bertambahnya waktu proses, penggunaan CPU, dan konsumsi RAM. Efisiensi dekripsi bervariasi tergantung pada algoritma yang digunakan dan jenis file yang diproses.

Tabel 4. Ringkasan Rata-rata Proses Dekripsi

Tipe *File*	**Ukuran Acuan**	**Waktu Proses (s)**		***CPU Usage (%)***		***RAM Usage (MB)***	
		Camellia	**AES**	**Camellia**	**AES**	**Camellia**	**AES**
*.mp3	100 KB	282.39	78.89	24.82	23.50	29.72	21.49
	1024 KB	441.79	138.52	25.53	25.53	32.07	23.59
	10240 KB	630.44	268.60	27.50	27.51	33.57	24.48
*.jpg	100 KB	181.40	96.32	18.64	21.24	21.16	19.50
	1024 KB	240.79	154.13	21.17	23.44	24.41	23.44
	10240 KB	320.44	275.45	23.58	24.60	25.57	26.66
*.png	100 KB	121.40	73.74	28.31	21.22	23.16	23.58
	1024 KB	300.79	144.99	32.17	24.57	26.07	25.64
	10240 KB	530.44	208.12	34.59	26.29	26.90	26.64
*.pdf	100 KB	181.40	107.08	33.98	25.71	32.49	29.79
	1024 KB	340.79	325.69	35.17	29.50	35.74	32.22
	10240 KB	510.44	504.91	39.59	34.29	37.90	33.23
*.docx	100 KB	121.40	121.40	22.64	21.95	21.16	22.78
	1024 KB	260.79	219.12	24.17	25.55	23.74	24.73
	10240 KB	390.44	442.44	29.59	28.48	24.57	25.56
*.xls	100 KB	121.40	131.40	28.31	24.31	23.49	23.15
	1024 KB	230.79	277.45	30.50	28.84	24.74	24.07
	10240 KB	410.44	440.11	34.59	31.25	26.57	25.57
*.pptx	100 KB	131.40	131.40	24.98	24.31	26.16	23.49
	1024 KB	200.79	277.45	28.50	25.50	28.74	25.74
	10240 KB	330.44	440.11	30.59	29.59	31.56	27.90
*.txt	100 KB	121.40	131.40	24.64	28.64	23.16	28.49
	1024 KB	220.79	210.78	27.50	30.50	27.74	30.56
	10240 KB	410.44	330.44	31.92	32.59	30.57	32.74



Gambar 5. Visualisasi Parameter Dekripsi

Evaluasi terhadap proses enkripsi dan dekripsi menunjukkan perbedaan kinerja yang konsisten antara algoritma Camellia dan AES pada berbagai jenis file dan ukuran yang telah ditentukan (100 KB, 1024 KB, dan 10240 KB). Pada tahap enkripsi, AES secara konsisten menghasilkan waktu proses yang lebih cepat. Sebagai contoh, untuk mengenkripsi file *.mp3 berukuran 10 MB, AES hanya membutuhkan 217,75 detik, sedangkan Camellia memerlukan 646,16 detik—hampir tiga kali lebih lama. Pola serupa juga terlihat pada file *.pdf, di mana AES memproses ukuran terbesar dalam 340,52 detik, sementara Camellia membutuhkan 392,14 detik. Namun, kecepatan ini sering kali disertai dengan penggunaan memori yang lebih tinggi. Pada file *.pdf berukuran 10 MB, enkripsi menggunakan AES mengonsumsi 35,03 MB RAM, sementara Camellia hanya menggunakan 27,99 MB. Pola serupa ditemukan pada format lain seperti *.xls dan *.jpg, di mana AES secara konsisten memerlukan lebih banyak memori selama proses enkripsi. Camellia umumnya menunjukkan beban CPU yang lebih tinggi saat proses enkripsi, terutama untuk file berukuran besar. Sebagai contoh, untuk mengenkripsi file *.png berukuran 10 MB, Camellia menggunakan 24,32% CPU, sementara AES membutuhkan 29,04%. Meski begitu, pola ini bervariasi tergantung format file. Pada file *.docx, misalnya, AES menunjukkan efisiensi CPU yang sedikit lebih baik dengan penggunaan sebesar 30,49%, dibandingkan Camellia yang menggunakan 28,81%.

Pada tahap dekripsi, AES kembali menunjukkan waktu pemrosesan yang lebih cepat. Untuk mendekripsi file *.png berukuran 10 MB, AES memerlukan 208,12 detik, sedangkan Camellia membutuhkan 530,44 detik. Dari sisi penggunaan RAM, Camellia umumnya lebih efisien. Sebagai contoh, untuk file *.xls berukuran 10 MB, AES menggunakan 25,57 MB memori, sementara Camellia sedikit lebih banyak yaitu 26,57 MB—selisih yang relatif kecil. Sebaliknya, saat mendekripsi file *.pdf dengan ukuran yang sama, AES justru mengonsumsi lebih sedikit memori (33,23 MB) dibandingkan Camellia (37,90 MB). Perbedaan ini menunjukkan bahwa penggunaan memori dipengaruhi oleh ukuran dan jenis file, serta cara masing-masing algoritma memproses data secara internal.

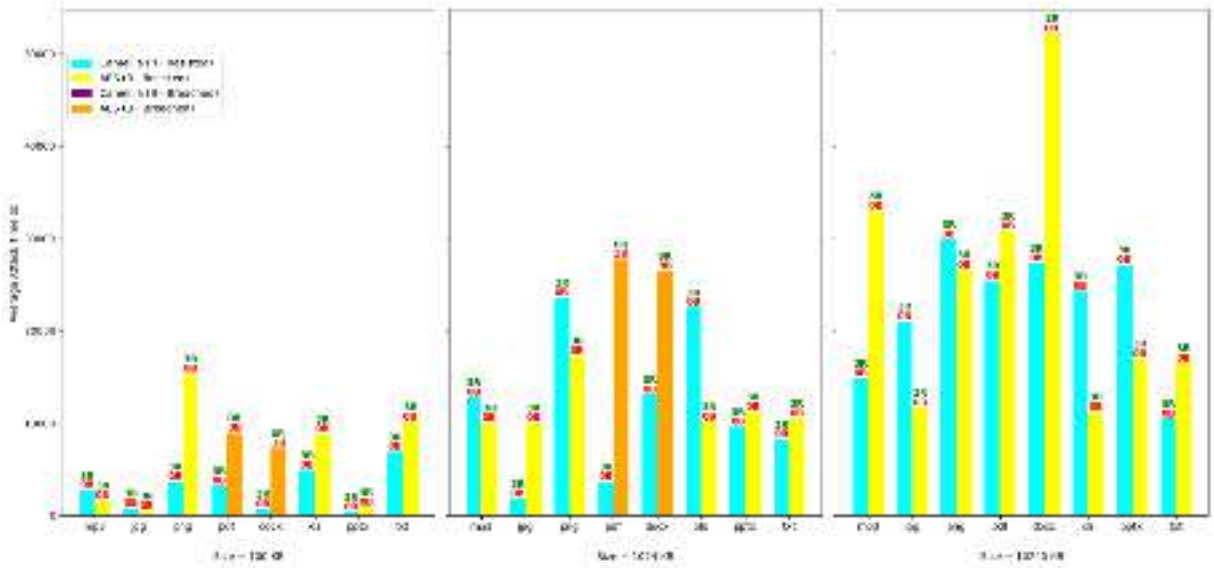
Selama tahap simulasi serangan, hasil yang diperoleh bervariasi tergantung pada jenis file, algoritma enkripsi, dan metode spesifik yang digunakan. Tabel 5 menyajikan hasil Uji *Dictionary Attack* untuk algoritma Camellia dan AES. Setiap entri mencantumkan *Attack Time* (AT) dalam satuan detik dan *Attack Outcomes* (AO), di mana 'R' menunjukkan bahwa enkripsi berhasil menahan serangan dan 'B' menandakan serangan berhasil menembus enkripsi.

Tabel 5. Hasil dari Pengujian *Dictionary Attack* Camellia dan AES

Tipe *File*	**Ukuran Acuan**	**File 1**				**File 2**				**File 3**			
		Camellia		**AES**		**Camellia**		**AES**		**Camellia**		**AES**	
		AT (s)	***AO***	***AT (s)***	***AO***	***AT (s)***	***AO***	***AT (s)***	***AO***	***AT (s)***	***AO***	***AT (s)***	***AO***
*.mp3	100 KB	2657	R	1587	R	2677	R	1617	R	2637	R	1577	R
	1024 KB	32751	R	10002	R	2765	R	10042	R	2735	R	9972	R
	10240 KB	14808	R	32801	R	14828	R	33051	R	14798	R	33051	R
*.jpg	100 KB	726	R	426	R	736	R	436	R	726	R	416	R
	1024 KB	1739	R	9957	R	1759	R	9917	R	1719	R	10117	R
	10240 KB	21019	R	11624	R	21039	R	11724	R	20999	R	11574	R
*.png	100 KB	3648	R	15301	R	3668	R	15341	R	3628	R	15281	R
	1024 KB	23552	R	17269	R	23582	R	17319	R	23532	R	17219	R
	10240 KB	29844	R	26569	R	29794	R	26656	R	29914	R	26556	R
*.pdf	100 KB	3160	R	8934	B	3180	R	8954	B	3140	R	8914	B
	1024 KB	3616	R	27722	B	3636	R	27692	B	3596	R	27772	B
	10240 KB	25445	R	30757	R	25475	R	30787	R	25425	R	30767	R
*.docx	100 KB	639	R	7200	B	659	R	7230	B	619	R	7180	B
	1024 KB	13063	R	26408	B	13083	R	26438	B	13043	R	26378	B
	10240 KB	27309	R	52224	R	27329	R	52194	R	27289	R	52294	R
*.xls	100 KB	4900	R	8757	R	4920	R	8787	R	4880	R	8727	R
	1024 KB	22510	R	10099	R	22540	R	10069	R	22470	R	10139	R
	10240 KB	24259	R	11160	R	24229	R	11190	R	24309	R	11130	R
*.pptx	100 KB	306	R	791	R	326	R	801	R	306	R	781	R
	1024 KB	9553	R	11150	R	9573	R	11180	R	9533	R	11130	R
	10240 KB	27111	R	16929	R	27131	R	16959	R	27091	R	16899	R
*.txt	100 KB	6858	R	10058	R	6878	R	10088	R	6838	R	10028	R
	1024 KB	8185	R	10482	R	8195	R	10512	R	8165	R	10482	R
	10240 KB	10426	R	16492	R	10446	R	16522	R	10406	R	16472	R

Tabel 5 menunjukkan bahwa algoritma Camellia secara konsisten mampu menahan semua upaya Dictionary Attack pada berbagai jenis dan ukuran file, tanpa satu pun kasus pelanggaran yang terjadi. Sebaliknya, AES menunjukkan kerentanan pada format tertentu, khususnya file *.pdf dan *.docx berukuran 100 KB dan 1024 KB. *Attack Time* bervariasi tergantung pada ukuran dan jenis file; misalnya, file kecil seperti *.pptx berukuran 100 KB menunjukkan durasi serangan tercepat, dengan Camellia menyelesaikan dalam 306–326 detik dan AES dalam 781–801 detik. Untuk file besar seperti *.pdf dan *.png berukuran 10240 KB, AES memerlukan lebih dari 30.000 detik, sedangkan Camellia tetap di bawah ambang tersebut. Variasi ini menunjukkan bahwa ukuran file dan struktur internal—seperti tingkat kompresi atau metadata—berpengaruh terhadap efektivitas serangan kamus. Gambar 6 memvisualisasikan rata-rata waktu serangan dari Tabel 5 untuk perbandingan yang lebih jelas antara kedua algoritma. Pengambilan rata-rata dianggap sah karena tiga nilai waktu serangan dalam setiap kasus uji sangat berdekatan, dan hasilnya konsisten, yaitu berupa resistensi penuh (3R) atau pelanggaran penuh (3B). Pola 3B, yang ditandai dengan hasil '0R 3B' (nol file menahan, tiga

file ditembus), hanya ditemukan pada AES untuk file *.pdf dan *.docx pada ukuran 100 KB dan 1024 KB, menandakan adanya kelemahan saat menangani format dokumen terstruktur. Sebaliknya, Camellia mempertahankan pola 3R pada semua pengujian, membuktikan ketahanannya terhadap serangan kamus serta efisiensinya di berbagai karakteristik file. Hasil ini menegaskan keunggulan Camellia dalam aspek keamanan terhadap metode *Dictionary Attack*. Dengan demikian, Camellia dapat dipertimbangkan sebagai algoritma yang lebih andal untuk melindungi data pada berbagai format dan ukuran file.



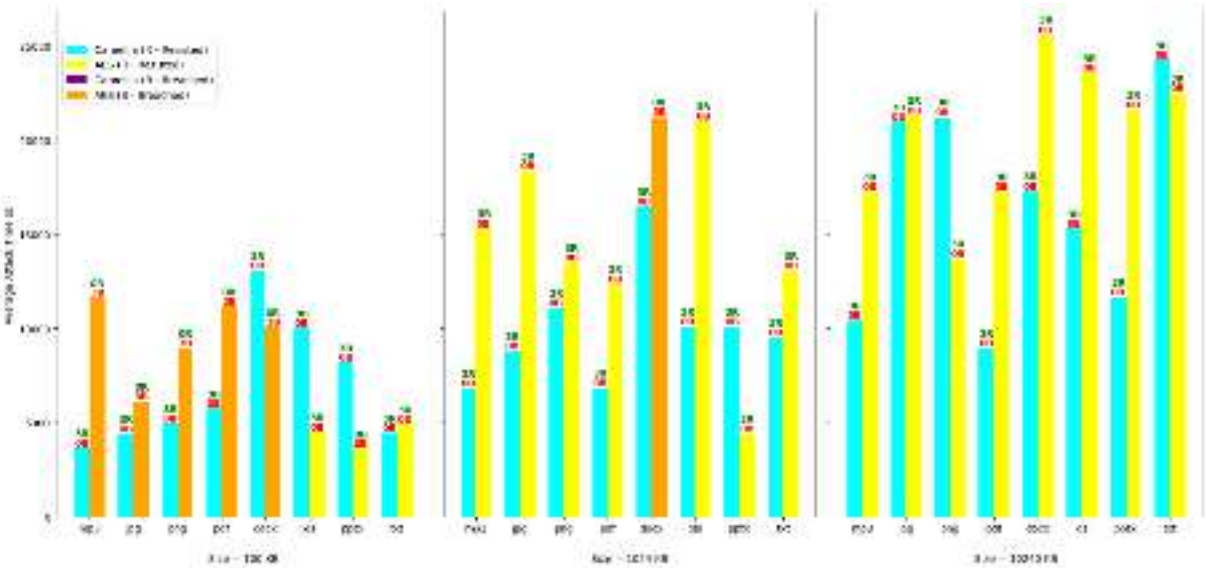
Gambar 6. Visualisasi *Dictionary Attack*

Tabel 6 menunjukkan bahwa algoritma Camellia secara konsisten mampu menahan semua upaya *Birthday Attack* pada setiap jenis dan ukuran file, tanpa terdeteksi adanya pelanggaran. Sebaliknya, AES berhasil ditembus dalam beberapa kasus, terutama pada file *.mp3, *.jpg, *.png, *.pdf, dan *.docx berukuran 100 KB serta *.docx berukuran 1024 KB. Waktu serangan bervariasi tergantung jenis dan ukuran file—file berukuran kecil seperti *.jpg dan *.mp3 pada 100 KB memiliki durasi serangan yang lebih singkat (sekitar 6100–11600 detik pada AES), sementara file besar seperti *.docx dan *.txt berukuran 10240 KB memerlukan waktu lebih dari 25.000 detik pada AES dan lebih dari 24.000 detik pada Camellia. Temuan ini menunjukkan bahwa meskipun Camellia menunjukkan ketahanan penuh, karakteristik file dan perilaku algoritma saat menghadapi serangan berbasis kolisi tetap memengaruhi beban komputasi yang dibutuhkan. Gambar 7 menggambarkan perbandingan ini secara visual dengan memaparkan rata-rata waktu serangan antara AES dan Camellia, berdasarkan tiga ukuran uji yang telah ditentukan secara konsisten. Data mengonfirmasi bahwa AES mengalami pelanggaran (3B) pada beberapa file kecil—terutama *.mp3, *.pdf, *.docx, dan *.txt berukuran 100 KB, serta *.docx pada 1024 KB—sedangkan Camellia mempertahankan ketahanan penuh (3R) pada seluruh file yang diuji. Menariknya, bahkan dalam kasus di mana kedua algoritma berhasil menahan serangan, AES tetap membutuhkan durasi lebih lama, dengan selisih waktu paling mencolok pada ukuran 10240 KB, menunjukkan bahwa Camellia tidak hanya tangguh, tetapi juga lebih efisien dalam menangani file berukuran besar. Keunggulan ini menjadikan Camellia sebagai pilihan yang lebih andal untuk menghadapi serangan kriptografi berbasis kolisi, dengan kombinasi ketahanan penuh dan efisiensi waktu yang menunjukkan performa

signifikan dibandingkan AES, serta memperkuat posisinya sebagai algoritma enkripsi yang lebih optimal untuk berbagai ukuran dan jenis file.

Tabel 6. Hasil dari Pengujian *Birthday Attack*

Tipe *File*	Ukuran Acuan	File 1				File 2				File 3			
		Camellia		AES		Camellia		AES		Camellia		AES	
		AT (s)	*AO*	*AT (s)*	*AO*	*AT (s)*	*AO*	*AT (s)*	*AO*	*AT (s)*	*AO*	*AT (s)*	*AO*
*.mp3	100 KB	3616	R	11624	B	3711	R	11634	B	3602	R	11604	B
	1024 KB	6858	R	15301	R	6768	R	15331	R	6804	R	15281	R
	10240 KB	10426	R	17269	R	10403	R	17229	R	10503	R	17299	R
*.jpg	100 KB	4400	R	6132	B	4344	R	6102	B	4435	R	6162	B
	1024 KB	8757	R	18370	R	8816	R	18340	R	8803	R	18400	R
	10240 KB	21019	R	21307	R	20969	R	21337	R	20965	R	21277	R
*.png	100 KB	4900	R	8934	B	4890	R	8964	B	4993	R	8904	B
	1024 KB	11150	R	13500	R	11060	R	13530	R	11075	R	13490	R
	10240 KB	21247	R	13699	R	21206	R	13729	R	21208	R	13669	R
*.pdf	100 KB	5733	R	11150	B	5772	R	11180	B	5721	R	11120	B
	1024 KB	6858	R	12342	R	6792	R	12372	R	6926	R	12312	R
	10240 KB	8934	R	17272	R	9018	R	17302	R	8927	R	17242	R
*.docx	100 KB	13063	R	10058	B	13044	R	10088	B	13069	R	10028	B
	1024 KB	16492	R	21247	B	16449	R	21277	B	16475	R	21217	B
	10240 KB	17269	R	25608	R	17309	R	25638	R	17280	R	25578	R
*.xls	100 KB	10002	R	4486	R	10076	R	4516	R	9930	R	4456	R
	1024 KB	10099	R	21019	R	10172	R	21049	R	10027	R	20989	R
	10240 KB	15301	R	23552	R	15347	R	23582	R	15209	R	23522	R
*.pptx	100 KB	8185	R	3616	R	8283	R	3586	R	8096	R	3646	R
	1024 KB	10077	R	4400	R	10098	R	4430	R	10055	R	4370	R
	10240 KB	11624	R	21622	R	11655	R	21652	R	11697	R	21592	R
*.txt	100 KB	4486	R	4900	R	4414	R	4930	R	4386	R	4870	R
	1024 KB	9553	R	13063	R	9457	R	13093	R	9590	R	13033	R
	10240 KB	24259	R	22510	R	24292	R	22540	R	24208	R	22480	R



Gambar 7. Visualisasi *Birthday Attack*

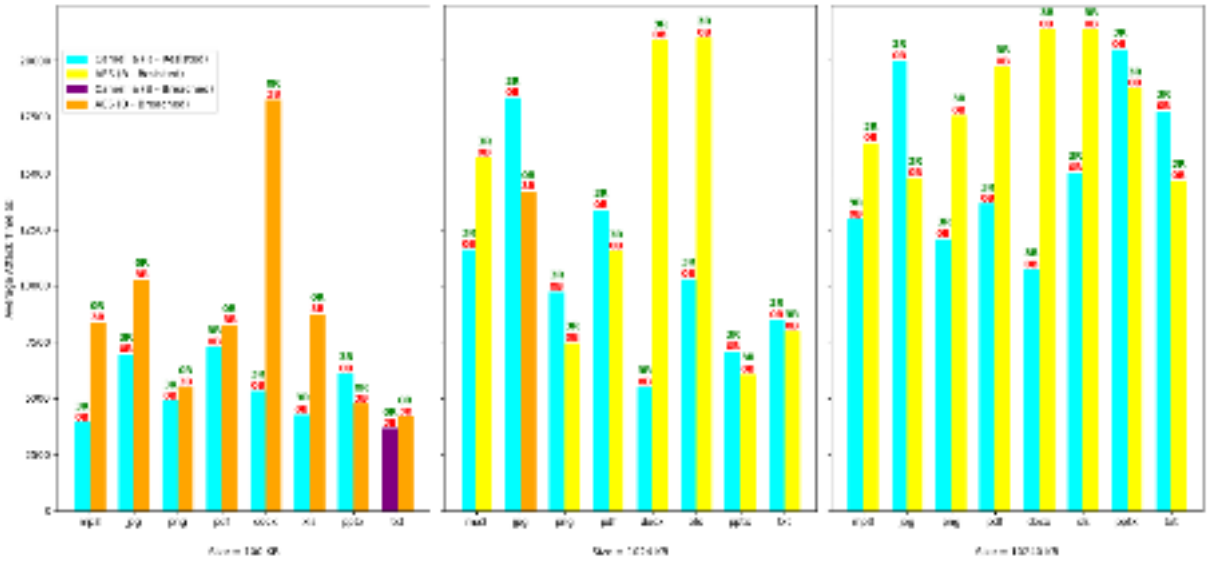
Tabel 7 mengungkapkan kontras kinerja yang jelas antara kedua algoritma, terutama pada level ukuran 100 KB yang menjadi titik kritis dalam pengujian. AES secara konsisten memerlukan durasi serangan yang lebih lama dibandingkan Camellia, dengan perbedaan mencolok terlihat pada file seperti *.docx, *.jpg, dan *.xls yang membutuhkan waktu lebih dari 18.000 detik untuk diserang. Di sisi lain, Camellia mampu mempertahankan waktu serangan yang lebih rendah dan menunjukkan hasil yang lebih stabil di berbagai jenis dan ukuran file, mencerminkan efisiensi komputasinya dalam menghadapi serangan brute-force. Ketika ukuran file meningkat hingga 10240 KB, kedua algoritma mengalami peningkatan durasi serangan, namun AES tetap menunjukkan performa yang lebih lambat secara keseluruhan. Pola ini mengindikasikan bahwa Camellia lebih unggul dalam menangani serangan brute-force, baik dari segi waktu maupun konsistensi, sementara beberapa file kecil berukuran 100 KB tampak lebih rentan terhadap serangan, terutama saat dienkripsi menggunakan AES. Hal ini semakin mempertegas keunggulan Camellia dalam skenario pengujian yang melibatkan berbagai tipe dan ukuran file.

Tabel 7. Hasil dari Pengujian *Brute-Force Attack*

Tipe *File*	**Ukuran Acuan**	**File 1**				**File 2**				**File 3**			
		Camellia		**AES**		**Camellia**		**AES**		**Camellia**		**AES**	
		AT (s)	***AO***	***AT (s)***	***AO***	***AT (s)***	***AO***	***AT (s)***	***AO***	***AT (s)***	***AO***	***AT (s)***	***AO***
*.mp3	100 KB	3943	R	8340	B	3900	R	8344	B	3843	R	8331	B
	1024 KB	11580	R	15720	R	11573	R	15604	R	11653	R	15663	R
	10240 KB	12960	R	16380	R	12983	R	16272	R	12892	R	16364	R
*.jpg	100 KB	6960	R	10260	B	6910	R	10373	B	6947	R	10111	B
	1024 KB	18360	R	14160	B	18302	R	14038	B	18361	R	14307	B
	10240 KB	19980	R	14760	R	19922	R	14746	R	20045	R	14858	R
*.png	100 KB	4860	R	5520	B	4886	R	5416	B	4805	R	5518	B
	1024 KB	9720	R	7440	R	9698	R	7538	R	9743	R	7350	R
	10240 KB	12060	R	17580	R	12057	R	17508	R	12099	R	17596	R
*.pdf	100 KB	7260	R	8220	B	7231	R	8188	B	7288	R	8303	B
	1024 KB	13380	R	11520	R	13356	R	11468	R	13346	R	11554	R
	10240 KB	13620	R	19680	R	13611	R	19670	R	13631	R	19812	R
*.docx	100 KB	5340	R	18240	B	5305	R	18210	B	5300	R	18296	B
	1024 KB	5460	R	20880	R	5471	R	20902	R	5479	R	20902	R
	10240 KB	10680	R	21022	R	10739	R	21600	R	10713	R	21517	R
*.xls	100 KB	4260	R	8760	B	4300	R	8727	B	4233	R	8718	B
	1024 KB	10320	R	21000	R	10226	R	21010	R	10299	R	21012	R
	10240 KB	15000	R	21420	R	15005	R	21336	R	15039	R	21437	R
*.pptx	100 KB	6120	R	4740	B	6031	R	4590	B	6101	R	4844	B
	1024 KB	7080	R	6000	R	7045	R	6105	R	7063	R	6024	R
	10240 KB	20520	R	18780	R	20462	R	18788	R	20478	R	18697	R
*.txt	100 KB	3660	B	4080	B	3661	B	4193	B	3595	B	4170	B
	1024 KB	8460	R	8040	R	8458	R	7911	R	8507	R	7945	R
	10240 KB	17760	R	14640	R	17782	R	14564	R	17712	R	14782	R

Gambar 7 menyajikan rata-rata waktu serangan brute-force untuk AES dan Camellia pada berbagai jenis dan ukuran file, berdasarkan hasil konsisten dari tiga file uji yang telah ditentukan untuk setiap tipe dan ukuran pada Tabel 7. Pada ukuran 100 KB, AES berhasil ditembus pada semua jenis file (0R 3B), termasuk file *.jpg, sementara Camellia menunjukkan ketahanan yang lebih kuat dengan hasil 3R 0B—kecuali pada file *.txt yang mencatatkan hasil

0R 3B. Untuk ukuran file yang lebih besar, kedua algoritma berhasil menahan seluruh serangan secara penuh (3R 0B di semua kasus), dengan waktu serangan yang meningkat seiring bertambahnya ukuran file. Hasil ini menunjukkan bahwa ketahanan terhadap serangan meningkat pada ukuran file yang lebih besar, sekaligus menyoroti adanya kerentanan spesifik pada algoritma Camellia terhadap file *.txt berukuran kecil. Temuan ini memperkuat pentingnya mempertimbangkan jenis file dalam evaluasi keamanan algoritma enkripsi.



Gambar 8. Visualisasi *Brute-Force Attack*

Yang penting untuk dicatat, tidak ada dari hasil tersebut yang disebabkan oleh batas waktu (*timeout*) atau batasan eksekusi. Kasus *breached* yang terjadi merupakan hasil dari keberhasilan penemuan kunci secara nyata selama simulasi, bukan akibat dari penghentian proses secara prematur atau alokasi waktu yang tidak mencukupi. Hal ini menegaskan bahwa ketahanan algoritma, bukan durasi pemrosesan, adalah faktor penentu utama dalam keberhasilan atau kegagalan serangan. Tabel 8 menyajikan total jumlah kasus *Resisted* (R) dan *Breached* (B) untuk masing-masing algoritma di seluruh jenis file dan tipe serangan, yang merangkum keseluruhan hasil dari simulasi serangan yang telah dilakukan.

Fase simulasi serangan menyoroti perbedaan mencolok dalam performa keamanan antara algoritma Camellia dan AES terhadap tiga jenis ancaman kriptografi yang umum. Pada Dictionary Attack, Camellia secara konsisten berhasil menahan semua upaya serangan di seluruh jenis dan ukuran file, sementara AES mengalami breached pada kasus tertentu—terutama file *.pdf dan .docx berukuran 100 KB dan 1024 KB—yang mengindikasikan kemungkinan kerentanan dalam pola derivasi kunci atau enkripsinya terhadap tebakan berbasis wordlist pada dokumen kecil atau terstruktur. Pada *Birthday Attack*, AES kembali menunjukkan kelemahan, dengan breached yang tercatat pada file seperti *.mp3, .jpg, .png, .pdf, dan .docx, khususnya pada ukuran kecil, sedangkan Camellia menahan seluruh pengujian, menunjukkan ketahanan yang lebih baik terhadap eksploitasi kolisi berbasis entropi. Pada Brute-Force Attack, AES gagal pada semua file berukuran 100 KB yang diuji, memperlihatkan kerentanan total pada ukuran kecil. Camellia lebih tangguh secara keseluruhan, namun tetap mengalami satu kasus breached pada file .txt 100 KB, yang menunjukkan bahwa struktur file yang sederhana dapat memperkecil jumlah permutasi kunci yang dibutuhkan untuk mencocokkan plaintext, sehingga meningkatkan efektivitas serangan brute-force dalam kondisi

tertentu. Temuan ini secara keseluruhan menegaskan keunggulan Camellia dalam menghadapi beragam skenario serangan kriptografi dibandingkan AES, dan dengan demikian, Camellia dapat dianggap sebagai algoritma yang lebih andal untuk perlindungan data pada berbagai format dan ukuran file.

Tabel 8. Ringkasan *Attack Outcomes*

Tipe *File*	**Ukuran Acuan**	***Dictionary Attack***				***Birthday Attack***				***Brute-Force Attack***				**Total**	
		Camellia		**AES**		**Camellia**		**AES**		**Camellia**		**AES**			
		B	**R**	**B**	**R**	**B**	**R**	**B**	**R**	**B**	**R**	**B**	**R**	**B**	**R**
*.mp3	100 KB	0	3	0	3	0	3	3	0	0	3	3	0	**6**	**12**
	1024 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
	10240 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
*.jpg	100 KB	0	3	0	3	0	3	3	0	0	3	3	0	**6**	**12**
	1024 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
	10240 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
*.png	100 KB	0	3	0	3	0	3	3	0	0	3	3	0	**6**	**12**
	1024 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
	10240 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
*.pdf	100 KB	0	3	3	0	0	3	3	0	0	3	3	0	**9**	**9**
	1024 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
	10240 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
*.docx	100 KB	0	3	3	0	0	3	3	0	0	3	3	0	**9**	**9**
	1024 KB	0	3	3	0	0	3	3	0	0	3	0	3	**6**	**12**
	10240 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
*.xls	100 KB	0	3	0	3	0	3	0	3	0	3	3	0	**3**	**15**
	1024 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
	10240 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
*.pptx	100 KB	0	3	0	3	0	3	0	3	0	3	3	0	**3**	**15**
	1024 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
	10240 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
*.txt	100 KB	0	3	0	3	0	3	0	3	3	0	3	0	**6**	**12**
	1024 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
	10240 KB	0	3	0	3	0	3	0	3	0	3	0	3	**0**	**18**
	Total	**0**	**72**	**9**	**63**	**0**	**72**	**18**	**54**	**3**	**69**	**24**	**48**	**54**	**378**

Perbandingan performa antara Camellia dan AES mengungkap karakteristik yang berbeda dalam hal efisiensi komputasi dan ketahanan kriptografi. Pada fase enkripsi dan dekripsi, AES secara konsisten menunjukkan kecepatan yang lebih tinggi, menyelesaikan proses dalam waktu yang jauh lebih singkat dibandingkan Camellia untuk semua jenis dan ukuran file. Keunggulan ini terutama terlihat pada file berukuran besar, di mana AES mampu memproses hampir tiga kali lebih cepat, menjadikannya lebih sesuai untuk aplikasi yang menuntut efisiensi waktu. Namun, kecepatan ini dibayar dengan konsumsi memori yang lebih tinggi. AES umumnya menggunakan lebih banyak RAM selama proses enkripsi, terutama pada file kompleks seperti *.pdf dan *.xls. Sebaliknya, Camellia menunjukkan penggunaan memori yang lebih stabil dan rendah, yang mengindikasikan keunggulannya dalam lingkungan dengan keterbatasan sumber daya. Penggunaan CPU bervariasi tergantung pada jenis file, meskipun Camellia cenderung menghasilkan beban prosesor sedikit lebih tinggi saat enkripsi, sementara AES lebih efisien pada format tertentu seperti *.docx. Dalam hal ketahanan terhadap serangan, fase simulasi menunjukkan kelemahan relatif pada AES dibandingkan Camellia. Camellia berhasil menahan

semua serangan pada kategori Dictionary dan Birthday, dan hanya mengalami satu kasus breached pada pengujian Brute-Force (file *.txt 100 KB). Sebaliknya, AES mencatat beberapa kasus breached, terutama pada file berukuran kecil. AES gagal mempertahankan keamanan terhadap serangan Dictionary dan Birthday pada format seperti *.pdf dan *.docx di ukuran 100 KB dan 1024 KB, serta gagal pada semua tipe file dalam serangan Brute-Force pada ukuran terkecil. Meskipun unggul dalam kecepatan, temuan ini menunjukkan bahwa AES mungkin kurang tahan terhadap teknik kriptanalisis tertentu, khususnya pada file kecil atau terstruktur. Sebaliknya, Camellia menawarkan perlindungan yang lebih konsisten, terutama pada ukuran file kecil, meskipun dengan kecepatan yang sedikit lebih rendah.

Variasi yang diamati pada waktu proses, penggunaan CPU, dan konsumsi memori menegaskan bahwa karakteristik performa kedua algoritma sangat bergantung pada jenis file dan skala beban kerja. Seiring meningkatnya ukuran file, perbedaan antara AES dan Camellia menjadi semakin mencolok, memberikan wawasan berharga mengenai kecocokan masing-masing algoritma terhadap kebutuhan sistem dan lingkungan pemrosesan yang berbeda. Simulasi serangan juga memperlihatkan perbedaan signifikan dalam respons masing-masing algoritma terhadap ancaman kriptografi. Tingkat resistensi bervariasi pada skenario Dictionary, Birthday, dan Brute-Force, bergantung pada struktur dan ukuran file. Sementara AES menunjukkan banyak breached—terutama pada file kecil dan terstruktur—Camellia secara konsisten memperlihatkan ketahanan yang lebih kuat dalam sebagian besar kasus, menandakan perlindungan bawaan yang lebih tangguh di berbagai kondisi.

Penilaian terhadap Camellia dan AES dilakukan berdasarkan gabungan aspek efisiensi performa dan ketahanan kriptografi. Alih-alih mengunggulkan salah satu algoritma secara mutlak, temuan ini menekankan pentingnya menyelaraskan pemilihan algoritma dengan prioritas sistem. Satu algoritma mungkin memberikan keunggulan operasional untuk aplikasi dengan kebutuhan pemrosesan cepat, sementara algoritma lain dapat menawarkan ketahanan lebih konsisten dalam skenario yang mengutamakan keamanan terhadap serangan berkelanjutan. Hasil ini menegaskan bahwa kompromi antara performa dan keamanan tidak bersifat seragam di semua jenis atau ukuran file, sehingga keputusan dalam penerapan kriptografi perlu mempertimbangkan konteks penggunaan secara spesifik. Selain itu, kerentanan yang muncul pada file terstruktur tertentu menunjukkan bahwa penyempurnaan lebih lanjut atau strategi enkripsi hibrida mungkin diperlukan dalam praktik nyata.

BAB IV. KESIMPULAN DAN SARAN

Studi ini menyajikan analisis perbandingan performa antara algoritma Camellia dan AES pada berbagai jenis dan ukuran file. AES secara konsisten menunjukkan waktu enkripsi dan dekripsi yang lebih cepat, terutama pada file berukuran besar, menjadikannya cocok untuk aplikasi yang membutuhkan pemrosesan cepat. Namun, keunggulan kecepatan ini diimbangi dengan konsumsi memori yang lebih tinggi serta kerentanan terhadap serangan kriptanalisis. Di sisi lain, Camellia menunjukkan penggunaan sumber daya yang lebih stabil dan ketahanan yang lebih tinggi terhadap serangan, dengan hanya satu kasus breached yang tercatat pada pengujian brute-force terhadap file plaintext kecil. Sebaliknya, AES mengalami beberapa breached dalam skenario serangan dictionary dan birthday. Oleh karena itu, pemilihan algoritma sebaiknya disesuaikan dengan keterbatasan sistem dan tingkat keamanan yang dibutuhkan. AES direkomendasikan untuk lingkungan dengan kebutuhan pemrosesan cepat, sementara Camellia lebih tepat digunakan pada sistem yang mengutamakan keamanan dan efisiensi sumber daya. Penelitian selanjutnya disarankan untuk mencakup pengujian terhadap algoritma tambahan, memperluas variasi file, mengevaluasi performa dalam kondisi operasional waktu nyata, serta mempertimbangkan strategi enkripsi hibrida yang menggabungkan keunggulan beberapa algoritma guna mencapai keseimbangan optimal antara kecepatan, efisiensi, dan ketahanan dalam perlindungan data modern.

DAFTAR PUSTAKA

[1] Manullang S. Implementasi Kriptografi Pengamanan Data File Dokumen Menggunakan Algoritma Advanced Encryption Standard Mode Chiper Block Chaining. Jurnal Nasional Teknologi Komputer 2023;3. https://doi.org/10.61306/jnastek.v3i2.69.

[2] Matsui M, Moriai S, Nakajima J. RFC 3713 - A Description of the Camellia Encryption Algorithm 2015. https://datatracker.ietf.org/doc/rfc3713/ (accessed April 18, 2025).

[3] Azhari M, Mulyana DI, Perwitosari FJ, Ali F. Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer 2022;2. https://doi.org/10.47709/jpsk.v2i01.1390.

[4] Sulaiman AS, Hammood MM. Enhancing Data Security by Using Hybrid Encryption Technique Based on AES and Camellia. Learning and Analytics in Intelligent Systems 2025;45:173–82. https://doi.org/10.1007/978-3-031-82706-8_18.

[5] Shareef FR. A novel crypto technique based ciphertext shifting. Egyptian Informatics Journal 2020;21. https://doi.org/10.1016/j.eij.2019.11.002.

[6] Balaraju J, Rao PR, Biksham V, Prasada Rao PVRD, Tumuluru P. Dynamic Password to Enforce Secure Authentication Using DNA. International Journal of Intelligent Systems and Applications in Engineering 2024;12.

[7] Adams C. Dictionary Attack. Encyclopedia of Cryptography, Security and Privacy 2021:1–2. https://doi.org/10.1007/978-3-642-27739-9_74-2.

[8] Alkhwaja I, Albugami M, Alkhwaja A, Alghamdi M, Abahussain H, Alfawaz F, et al. Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming. Applied Sciences 2023;13:5979. https://doi.org/10.3390/app13105979.

[9] Hranický R, Šírová L, Rucký V. Beyond the dictionary attack: Enhancing password cracking efficiency through machine learning-induced mangling rules. Forensic Science International: Digital Investigation 2025;52:301865. https://doi.org/10.1016/j.fsidi.2025.301865.

[10] Chavan GT, Agrawal S, Sakhare NN, Mondal D, Vigenesh M, G V. Investigating the Effectiveness of Birthday Attack Strategies in Cryptography Network Security. 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), IEEE; 2023, p. 1–6. https://doi.org/10.1109/SMARTGENCON60755.2023.10442248.

[11] Fahdi H Al, Ahmed M. Cryptographic Attacks, Impacts and Countermeasures. Security Analytics for the Internet of Everything 2020:215–30. https://doi.org/10.1201/9781003010463-13.

[12] Ningrum DF, Tahir M, Angelina WD, Permatasari E, Rofiq FR, Hidayati M, et al. Implementasi Keamanan Data menggunakan Kriptografi Caesar Chiper. Jurnal Adijaya Multidisiplin (JAM) 2023;1.

[13] Triono A, Budi AS, Abdillah R. Implementasi Peretasan Sandi Vigenere Chipper Menggunakan Bahasa Pemograman Python. Jurnal JOCOTIS - Journal Science Informatika and Robotics 2023;1.

[14] Ali Hamza A, Jumma surayh Al-Janabi R. Detecting Brute Force Attacks Using Machine Learning. BIO Web Conf 2024;97:00045. https://doi.org/10.1051/bioconf/20249700045.

[15] Verma R, Dhanda N, Nagar V. Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms. Lecture Notes in Networks and Systems 2022;376:513–22. https://doi.org/10.1007/978-981-16-8826-3_44.

[16] Nair V, Song D. Multi-Factor Credential Hashing for Asymmetric Brute-Force Attack Resistance. 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), IEEE; 2023, p. 56–72. https://doi.org/10.1109/EuroSP57164.2023.00013.

[17] Sarmila KB, Manisekaran S V. Honey Encryption and AES based Data Protection Against Brute Force Attack. 6th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2022 - Proceedings, 2022. https://doi.org/10.1109/I-SMAC55078.2022.9987304.

[18] Ady Putra W, Suyanto S, Zarlis M. Performance Analysis Of The Combination Of Advanced Encryption Standard Cryptography Algorithms With Luc For Text Security. SinkrOn 2023;8. https://doi.org/10.33395/sinkron.v8i2.12202.

[19] Bibiola F, Kalsum TU, Alamsyah H. Penerapan Algoritma Advance Encryption Standard (AES) Untuk Pengamanan File Pada Aplikasi Berbasis WEB. JURNAL SURYA ENERGY 2023;8. https://doi.org/10.32502/jse.v8i1.6461.

[20] Li Y, Wang Q, Huang D, Liu J, Xie H. Quantum Chosen-Cipher Attack on Camellia. Cryptology EPrint Archive 2024.

[21] Nithishma A, Vijayan A, Nanda D, Kumar ChA, Thaseen S, Ahmad A. Remote User Authentication Using Camellia Encryption for Network-Based Applications. Security and Privacy-Preserving Techniques in Wireless Robotics 2022:255–79. https://doi.org/10.1201/9781003156406-19.

[22] Rasheed A, Baza M, Khan M, Karpoor N, Varol C, Srivastava G. Using Authenticated Encryption for Securing Controller Area Networks in Autonomous Mobile Platforms. International Symposium on Wireless Personal Multimedia Communications, WPMC, 2023. https://doi.org/10.1109/WPMC59531.2023.10338834.

[23] Li ZQ, Gao F, Qin SJ, Wen QY. Quantum circuit for implementing Camellia S-box with low costs. Scientia Sinica: Physica, Mechanica et Astronomica 2023;53. https://doi.org/10.1360/SSPMA-2022-0485.

[24] Mohammed AA, Rahma AMS, AbdulWahab HB. Security Encryption Model of E-bank Based Camellia Algorithm using Cubic Curve. AIP Conf Proc 2025;3264. https://doi.org/10.1063/5.0263610/3338501.

[25] Rashidi B. Flexible and high-throughput structures of Camellia block cipher for security of the Internet of Things. IET Comput Digit Tech 2021;15:171–84. https://doi.org/10.1049/CDT2.12025.

[26] Haris M, Lydia MS, Sutarman S. Pengamanan Pada Citra Digital dengan Menggunakan Modifikasi Blok Data Algoritma AES - Rijndael. JURNAL MEDIA INFORMATIKA BUDIDARMA 2023;7. https://doi.org/10.30865/mib.v7i1.5458.

[27] Tanjung PY. Penerapan Algoritma Aes 625 Dalam Pengamanan Data Rekam Medis. Journal Global Technology Computer 2022;1. https://doi.org/10.47065/jogtc.v1i3.2054.

[28] Andriyanto MR, Sukmasetya P. Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. Journal of Computer System and Informatics (JoSYC) 2022;4. https://doi.org/10.47065/josyc.v4i1.2451.

[29] Aulia A, Gunawan H. Penerapan Algoritma Advanced Encryption Standard Untuk Mengamankan File Gambar Pada Layanan Berbasis Web. Data Teknologi : Journal of Informatics and Computers 2023;1. https://doi.org/10.56248/datateknologi.v1i1.49.

[30] Dwina N, Khairani N, Nasir M, Indrawati I. Penerapan Metode Advanced Encryption Standard pada Sistem Penyimpanan Data Menggunakan Cloud Computing Sebagai Software-as-a-Service. Journal of Artificial Intelligence and Software Engineering (J-AISE) 2023;3. https://doi.org/10.30811/jaise.v3i1.4183.

[31] Putra Ramadani Tarigan A, Ramadhan PS, Ibnutama K. Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard). Jurnal Cyber Tech 2023;5. https://doi.org/10.53513/jct.v5i1.7851.

[32] Linda H, Sitorus SH, Ristian U. PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES)-128 BIT PADA KEAMANAN DATABASE APLIKASI KEPELANGGANAN (STUDI KASUS: PERUMDA AIR MINUM TIRTA KHATULISTIWA). Coding Jurnal Komputer Dan Aplikasi 2023;11. https://doi.org/10.26418/coding.v11i1.58122.

[33] Dani Saputro M, Wicaksana B, Zayid F. Penerapan Algoritma AES 256 Pada Qr Code Untuk Sistem Registrasi Event Sepeda. TeknoIS : Jurnal Ilmiah Teknologi Informasi Dan Sains 2023;13. https://doi.org/10.36350/jbs.v13i2.205.

[34] F R, Anwar A. Implementasi Kriptografi Dengan Metode Advanced Encryption Standard (AES) Untuk Realtime Chat Berbasis Mobile Pada E-Learning Politeknik Negeri Lhokseumawe. Journal of Artificial Intelligence and Software Engineering (J-AISE) 2021;1. https://doi.org/10.30811/jaise.v1i2.2520.

[35] Khusaeri Andesa, Afnand Fachzevi, Torkis Nasution, Herwin. Implementasi Metode AES pada Aplikasi Chat Menggunakan Flutter. SATIN - Sains Dan Teknologi Informasi 2023;9. https://doi.org/10.33372/stn.v9i2.1075.

[36] Rachmayanti A, Wirawan W. Implementasi Algoritma Advanced Encryption Standard (AES) pada Jaringan Internet of Things (IoT) untuk Mendukung Smart Healthcare. Jurnal Teknik ITS 2022;11. https://doi.org/10.12962/j23373539.v11i3.97042.

[37] Wei Z, Sun S, Hu L, Wei M, Peralta R. Searching the space of tower field implementations of the F28 inverter – with applications to AES, Camellia and SM4. International Journal of Information and Computer Security 2023;20. https://doi.org/10.1504/ijics.2023.127999.

[38] Hidayati LN, Fitriana GF, Adam IF. Perbandingan Keacakan Citra Enkripsi Algoritma AES dan Camelia Uji NPCR dan UACI. JURIKOM (Jurnal Riset Komputer) 2021;8. https://doi.org/10.30865/jurikom.v8i6.3624.

[39] Panahi U, Bayılmış C. Enabling secure data transmission for wireless sensor networks based IoT applications. Ain Shams Engineering Journal 2023;14. https://doi.org/10.1016/j.asej.2022.101866.

[40] Arabul E, Oliveira RD, Emami A, Typos S, Vrontos C, Wang R, et al. 100 Gbps quantum-secured and O-RAN-enabled programmable optical transport network for 5G fronthaul. Journal of Optical Communications and Networking 2023;15. https://doi.org/10.1364/JOCN.483644.

[41] Rasheed A, Baza M, Badr MM, Alshahrani H, Choo KKR. Efficient Crypto Engine for Authenticated Encryption, Data Traceability, and Replay Attack Detection Over CAN Bus Network. IEEE Trans Netw Sci Eng 2024;11. https://doi.org/10.1109/TNSE.2023.3312545.

[42] Muthavhine KD, Sumbwanyambe M. Blocking Linear Cryptanalysis Attacks Found on Cryptographic Algorithms Used on Internet of Thing Based on the Novel Approaches of Using Galois Field (GF (232)) and High Irreducible Polynomials. Applied Sciences (Switzerland) 2023;13. https://doi.org/10.3390/app132312834.

[43] Ning L, Ali Y, Ke H, Nazir S, Huanli Z. A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things. IEEE Access 2020;8. https://doi.org/10.1109/ACCESS.2020.3041327.

[44] Ali AK. THE IMPACT OF BLOCK AND STREAM CIPHER ON SESSION INITIATION PROTOCOL PROXY PERFORMANCE. Journal of Engineering Science and Technology 2022;17.

[45] Roy I, Rebeiro C, Hazra A, Bhunia S. SAFARI: Automatic synthesis of fault-attack resistant block cipher implementations. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2020;39. https://doi.org/10.1109/TCAD.2019.2897629.

[46] Hasan R, Khizar Y, Mahmood S, Sheikh MK. Design Space Exploration for High-Speed Implementation of the MISTY1 Block Cipher. Math Probl Eng 2021;2021. https://doi.org/10.1155/2021/2599500.

[47] Housley R, Schaad J. RFC 3394 - Advanced Encryption Standard (AES) Key Wrap Algorithm 2020. https://datatracker.ietf.org/doc/rfc3394/ (accessed April 18, 2025).

[48] Kato A, Moriai S. RFC 3657 - Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS) 2013. https://datatracker.ietf.org/doc/rfc3657/ (accessed April 18, 2025).

[49] Patra R, Patra S. Cryptography: A Quantitative Analysis of the Effectiveness of Various Password Storage Techniques. Journal of Student Research 2021;10. https://doi.org/10.47611/jsrhs.v10i3.1764.

[50] Montiel AH, Martínez AF, Jacinto GE. Implementation of Password Hashing on Embedded Systems with Cryptographic Acceleration Unit. International Journal of Advanced Computer Science and Applications 2022;13. https://doi.org/10.14569/IJACSA.2022.0130221.

[51] G EJ, A HM, S FHM. Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography. International Journal of Advanced Computer Science and Applications 2022;13. https://doi.org/10.14569/ijacsa.2022.01308104.

LAMPIRAN

Lampiran 1. Realisasi Penggunaan Anggaran

Dana Disetujui: Rp. 7.500.000,00

Jenis Pembelanjaan	Komponen	Item	Kuantitas	Biaya Satuan	Total
Belanja Bahan	ATK	- Spidol	6	15.000	90.000
		- Kertas A4	1	44.000	44.000
		- Pena	6	5.000	30.000
		- Materai	6	10.000	60.000
Belanja Bahan	Bahan penelitian (habis pakai)	- Akses Internet 2 org, 3 bulan	6	111.000	666.000
		- *Flashdisk*	2	235.000	470.000
Pengumpulan Data	Honor pembantu peneliti	- 1 org, 16 jam	16	25.000	400.000
Pengumpulan Data	FGD	- 2 org, 1 bln	2	225.000	450.000
Pengumpulan Data	Transport	- 2 org, 3x	6	50.000	300.000
Pengumpulan Data	Konsumsi	- 2 org, 3x	6	75.000	450.000
Analisis Data	Konsumsi	- 2 org, 3x	6	75.000	450.000
Analisis Data	Honor pengolah data	- 1 org, 6x	6	40.000	240.000
Analisis Data	Honor narasumber	- konsultasi	1	700.000	700.000
Sewa Peralatan	Peralatan penelitian	- laptop	1	250.000	250.000
Pelaporan penelitian	Honor administrasi peneliti	- 1 org, 2 bln	2	100.000	200.000
Lainnya	Biaya pendaftaran HKI	- 1 registrasi	1	200.000	200.000

Lampiran 2. Biodata Ketua dan Anggota Tim Peneliti

Ketua Tim Peneliti

A. Identitas Diri

1. Nama Lengkap (dengan gelar) : Teja Endra Eng Tju, S.T., M.Kom.
2. Jenis Kelamin : Pria
3. Jabatan Fungsional : Lektor
4. NIP/NIDN/ID-SINTA : 190046/0407127201/6713276
5. Tempat, Tanggal Lahir : Malang, 07 Desember 1972
6. E-mail : teja.endraengtju@budiluhur.ac.id
7. Nomor Handphone : +628998909707
8. Alamat : Alam Sutera, Tangerang Selatan

B. Riwayat Pendidikan

	S1	S2
Nama Perguruan Tinggi	ITS Surabaya	Universitas Budi Luhur
Bidang Ilmu	Teknik Telekomunikasi	Ilmu Komputer
Tahun Masuk-Lulus	1991 - 1996	2003 - 2009

C. Pengalaman Penelitian (5 Tahun Terakhir)

No.	Tahun	Judul Penelitian	Pendanaan	
			Sumber*	Jumlah (Rp)
1.	2025	Analisis Perbandingan Kinerja Algoritma Camellia dan AES	UBL	7.500.000,00
2.	2024	Optimalisasi Administrasi Pembayaran Sekolah dengan *Augmented Reality* dan *Payment Gateway*	UBL	5.000.000,00
3.	2024	Optimasi Pengalaman Berbelanja dengan Mengintegrasikan *Augmented Reality* dan *Payment Gateway* pada Storefront UKM	UBL	7.500.000,00
4.	2024	Optimalisasi Pengolahan Data VR Isyarat Tangan dengan Teknik Padding	Dikti	41.940.000,00
5.	2023	Pengolahan Data dari Pemanfaatan Perangkat Virtual Reality untuk Isyarat Tangan	UBL	13.300.000,00
6.	2023	Sistem Cerdas pada Aplikasi Pengenalan Bangun Datar untuk Siswa Taman Kanak-Kanak	Dikti	18.900.000,00
7.	2023	Identifikasi Cerdas Hoaks dengan Metode Naive Bayes dan Decision Tree	UBL	5.000.000,00

** Tuliskan sumber pendanaan baik dari Universitas Budi Luhur maupun dari sumber lainnya.*

D. Publikasi Artikel Ilmiah dalam Jurnal (5 Tahun Terakhir)

No.	Judul Artikel Ilmiah*	Nama Jurnal	Volume/ Nomor/ Tahun

1.	Hand Sign Virtual Reality Data Processing Using Padding Technique	INSYST	6/2/2024
2.	Optimizing Shopping Experience by Integrating Augmented Reality and Payment Gateway in SME Storefronts	MATICS	16/2/2024
3.	Hand Sign Interpretation through Virtual Reality Data Processing	JIKI	17/2/2024
4.	Pembangunan Fitur dalam Identifikasi Cerdas Hoaks dengan Naive Bayes dan Klasifikasi Decision Tree	Jutisi	13/1/2024
5.	Smart System on Two-dimensional Shapes Recognition Application for Kindergarten Students	SJI	11/1/2024
6.	Rancang Bangun Sistem Pelaporan Pemilihan Kepala Desa di Kementrian Dalam Negeri Indonesia	Kresna	3/1/2023
7.	Creation of Questionnaire Keywords with The CISE Method for KMS User Satisfaction Evaluation	Methomika	6/2/2022
8.	Naive Bayes dan Confusion Matrix untuk Efisiensi Analisa Intrusion Detection System Alert	Teknosi	8/2/2022
9.	Prediction of the COVID-19 Vaccination Target Achievement with Exponential Regression	JISA	4/2/2021

** Artikel ilmiah sebagai luaran dari kegiatan penelitian*

E. Pemakalah Seminar Ilmiah (5 Tahun Terakhir)

No.	Nama Temu Ilmiah/Seminar	Judul Artikel Ilmiah*	Waktu dan Tempat
-	-	-	-

** Artikel ilmiah sebagai luaran dari kegiatan penelitian*

F. Perolehan HKI (5 Tahun Terakhir)

No.	Judul/Tema HKI*	Tahun	Jenis	Nomor P/ID
1.	Metode Evaluasi Keamanan Siber Portal Akademik Berbasis OWASP Dan Threat Modeling	2025	Karya Tulis	EC00202505781/ 000845144
2.	Desain Aplikasi Administrasi Sekolah Dengan Integrasi Augmented Reality Dan Payment Gateway	2025	Karya Tulis	EC00202505779/ 000845142
3.	Kerangka Konsep Dan Diagram Alir Mekanisme Integrasi Augmented Reality Dan Payment Gateway Pada Storefront	2024	Karya Tulis	EC00202472013/ 000647363
4.	Motion Translator	2024	Program Komputer	EC00202411536/ 000586907
5.	"BENTUK BENDA" (BANGUN DATAR) Versi 1.0	2023	Program Komputer	EC00202382016/ 000514969

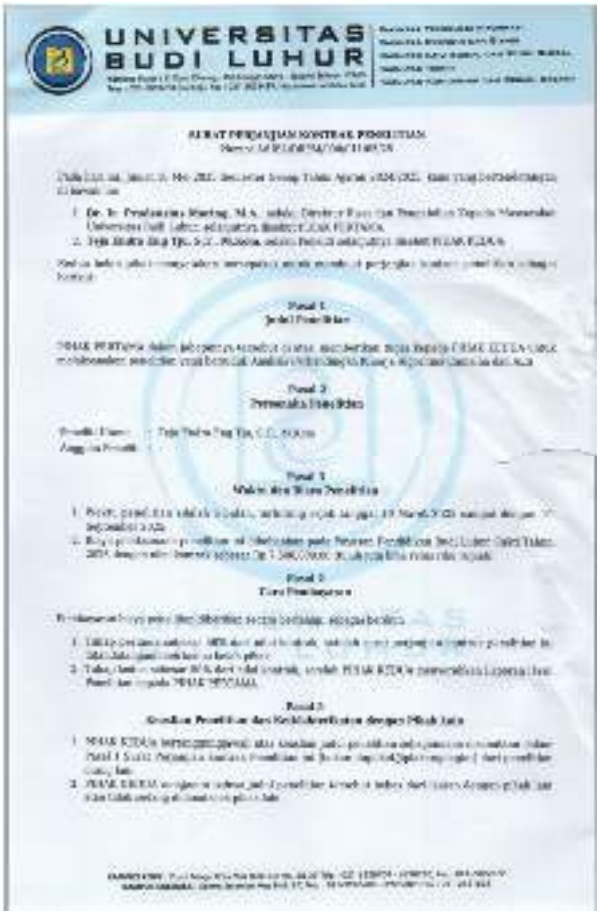
** HKI sebagai luaran dari kegiatan penelitian*

Jakarta, 01 Agustus 2025

Pengusul,

(Teja Endra Eng Tju, S.T., M.Kom.)

Lampiran 3. Surat Perjanjian Kontrak Penelitian



UNIVERSITAS BUDI LUHUR

SURAT PERJANJIAN KONTRAK PENELITIAN

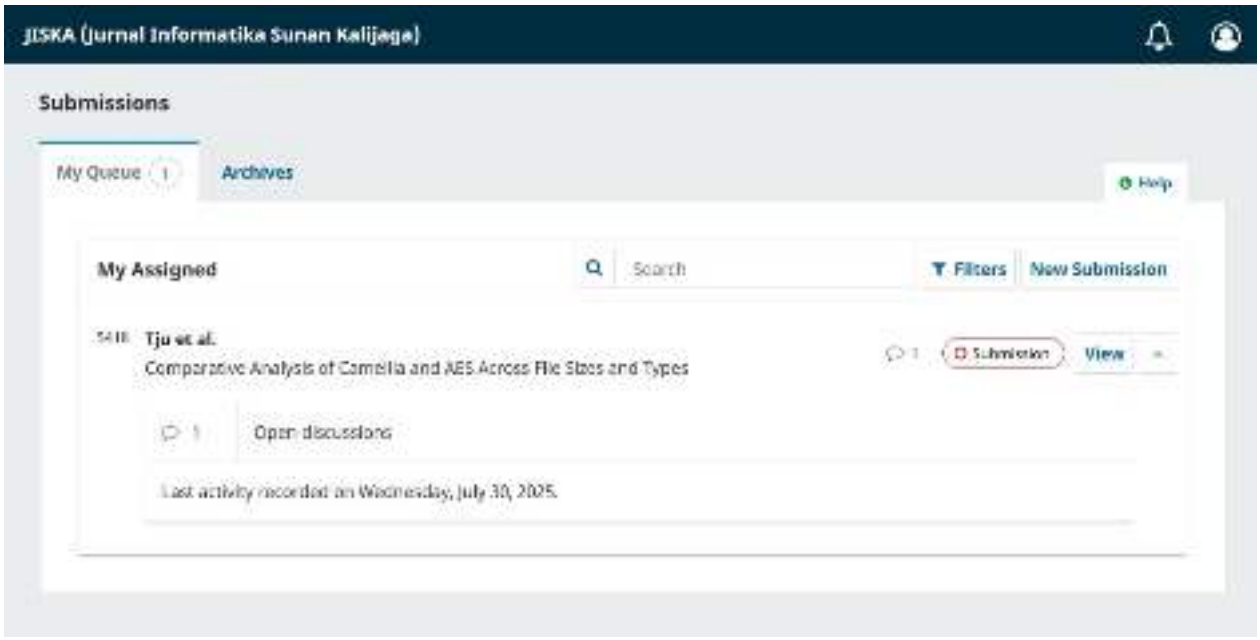
UNIVERSITAS BUDI LUHUR

UNIVERSITAS BUDI LUHUR

Lampiran 4. Catatan Harian

No	Tanggal	Kegiatan
1.	15/04/2025	Catatan: Sosialisasi pelaksanaan penelitian oleh DRPM
2.	16/04/2025	Catatan: Pengumpulan referensi jurnal artikel yang relevan
3.	18/04/2025	Catatan: Penyusunan kerangka konsep penelitian
4.	25/04/2025	Catatan: Pengusulan proposal penelitian
5.	28/04/2025	Catatan: Pengembangan aplikasi web untuk pengujian AES & Camellia
6.	16/05/2025	Catatan: Penandatanganan Kontrak Penelitian
7.	01/06/2025	Catatan: Melakukan pengumpulan dan persiapan data pengujian, yang terdiri dari 72 *file* dengan 8 jenis format
8.	07/06/2025	Catatan: Melakukan pengujian enkripsi dan dekripsi pada 72 *file*
9.	13/06/2025	Catatan: Melakukan simulasi *Dictionary Attack* untuk menguji ketahanan algoritma
10.	14/06/2025	Catatan: Melakukan simulasi *Birthday Attack* untuk menguji kerentanan probabilitas
11.	15/06/2025	Catatan: Melakukan simulasi *Brute-Force Attack* untuk menguji ketahanan absolut terhadap pencarian kunci
12.	18/06/2025	Catatan: Menganalisis kinerja dengan mengukur kecepatan proses, penggunaan CPU, dan memori
13.	21/06/2025	Catatan: Mengumpulkan dan menabulasi semua data hasil pengujian keamanan dan kinerja
14.	24/06/2025	Catatan: Mengevaluasi hasil untuk mengidentifikasi *trade-off* antara keamanan Camellia dan kecepatan AES
15.	27/06/2025	Catatan: Merumuskan kesimpulan dan rekomendasi pemilihan algoritma berdasarkan prioritas sistem
16.	04/07/2025	Catatan: Unggah laporan kemajuan di sistem DRPM Universitas Budi Luhur
17.	17/07/2025	Catatan: Pendaftaran HKI Model Perbandingan Efektivitas Algoritma
18.	25/07/2025	Catatan: Submit artikel ke Jurnal JISKa terakreditasi Sinta 3
19.	03/08/2025	Catatan: Penyerahan laporan akhir ke DRPM Universitas Budi Luhur

Lampiran 5. Artikel Ilmiah (*~~draft~~/submitted/~~reviewed/accepted/published~~*)



Lampiran 6. HKI

REPUBLIK INDONESIA
KEMENTERIAN HUKUM

SURAT PENCATATAN CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC002025064681, 17 Juli 2025
Pencipta		
Nama	:	**Teja Endra Eng Tju dan Fauzi Alfadhillah**
Alamat	:	Alam Sutera Suites III No. 12 A, RT.001/RW.009, Serpong Utara, Kota Tangerang Selatan, Banten, 15325
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**Direktorat Riset dan Pengabdian kepada Masyarakat Universitas Budi Luhur**
Alamat	:	Jl. Ciledug Raya, RT.10/RW.1, Petukangan Utara, Pesanggrahan, Kota Adm. Jakarta Selatan, DKI Jakarta, 12260
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Karya Tulis**
Judul Ciptaan	:	**Model Perbandingan Efektivitas Algoritma Kriptografi Camellia dan AES**
Tanggal dan tempat diumumkan untuk pertama kali di Wilayah Indonesia atau di luar wilayah Indonesia	:	15 Juli 2025, di DKI Jakarta
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor Pencatatan	:	000981952

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n. MENTERI HUKUM
DIREKTUR JENDERAL KEKAYAAN INTELEKTUAL
u.b.
Direktur Hak Cipta dan Desain Industri

Agung Damarsasongko, SH., MH.
NIP. 19681226 199403 1001