TECHNOVATAR Jurnal Teknologi, Industri dan Informasi
Vol. 2, No. 3, Juli 2024, pp. 1 – 10
Open Access:
https://journal.awatarapublisher.com/index.php/technovatar
ISSN: 3031-8874, DOI: 10.61434/technovatar.v2i3.392

IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIJNDAEL UNTUK PENGAMANAN FILE DIGITAL

Ade Sutriyono[1*], Dimas Dwi Rianto[2], Fasya Mahesa[3], Indah Rizkika[4]
[1, 2, 3, 4] Program Studi Informatika, Fakultas Teknik, Institut Teknologi dan Kesehatan Mahardika, Cirebon, Indonesia

INFO ARTIKEL
Sejarah Artikel:
Diterima, 4 Juni 2024
Direvisi, 12 Juni 2024
Disetujui, 9 Juli 2024

KEYWORDS
Rijndael
Advanced Encryption Standard
Encryption
Decryption
Digital file security

ABSTRACT

Digital file exchange requires protection against unauthorized access while preserving file usability after decryption. This study implements Rijndael with a 256-bit key in Cipher Block Chaining (CBC) mode in a desktop application. Functional evaluation covers 15 files: five PDF documents, five JPEG images, and five MP3 audio files. Evaluation examines encryption, recovery after decryption, and displayed file sizes, complemented by a theoretical comparison of AES key lengths. All tested files were recovered for use in their respective applications. The reported file sizes remain unchanged at the displayed KB or MB precision; this finding does not establish zero overhead at the byte level. Theoretical analysis shows that longer keys increase the key-search space, but does not constitute a brute-force experiment. The implementation supports functional protection of the tested file formats. Byte-level integrity checks, detailed diffusion measurements, and documentation of key and initialization-vector handling are needed for a comprehensive security assessment.

This work is licensed under a Creative Commons Attribution 4.0 International License.

KATA KUNCI
Rijndael
AES
Enkripsi
Dekripsi
Keamanan file digital

CORRESPONDING AUTHOR
Ade Sutriyono
Program Studi Informatika, Fakultas Teknik, Institut Teknologi dan Kesehatan Mahardika
Jl. Taman Pemuda No. 2, Cirebon 45153, Jawa Barat, Indonesia
Email: ade.sutriyono@mahardika.ac.id

ABSTRAK

Pertukaran file digital memerlukan perlindungan terhadap akses tanpa izin dengan tetap mempertahankan kegunaan berkas setelah dekripsi. Penelitian ini mengimplementasikan Rijndael dengan kunci 256 bit dalam mode Cipher Block Chaining (CBC) pada aplikasi desktop. Evaluasi fungsional mencakup 15 berkas, yaitu lima dokumen PDF, lima gambar JPEG, dan lima berkas audio MP3. Evaluasi meliputi proses enkripsi, pemulihan setelah dekripsi, dan ukuran tampil berkas, disertai perbandingan teoretis variasi panjang kunci AES. Seluruh berkas uji dapat dipulihkan untuk digunakan pada aplikasi sesuai formatnya. Ukuran berkas tetap sama pada ketelitian tampilan KB atau MB; temuan ini tidak membuktikan overhead nol pada tingkat byte. Analisis teoretis menunjukkan bahwa kunci yang lebih panjang memperbesar ruang pencarian, tetapi bukan merupakan eksperimen brute-force. Implementasi mendukung pengamanan fungsional pada format berkas yang diuji. Pemeriksaan integritas biner, pengukuran difusi terperinci, serta dokumentasi pengelolaan kunci dan initialization vector diperlukan untuk penilaian keamanan menyeluruh.

PENDAHULUAN

Pertukaran dokumen, gambar, dan audio secara elektronik memerlukan perlindungan terhadap akses yang tidak berwenang. Enkripsi mengubah data asli (plainteks) menjadi data tersandi (cipherteks) untuk menjaga kerahasiaan informasi (Fadlan dkk., 2019). Keberhasilan dekripsi dan kemampuan membuka kembali berkas merupakan indikator fungsional aplikasi. Namun, kedua indikator tersebut belum membuktikan autentikasi atau ketahanan terhadap manipulasi. Karena itu, penelitian ini membedakan evaluasi fungsi aplikasi dari penilaian keamanan kriptografis.

Kriptografi kunci simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi. Advanced Encryption Standard (AES) merupakan bagian dari keluarga algoritma Rijndael yang dikembangkan oleh Vincent Rijmen dan Joan Daemen (Siringoringo, 2020). Dalam naskah ini, istilah AES merujuk pada Rijndael dengan blok 128 bit; panjang kunci yang digunakan aplikasi adalah 256 bit. Pemilihan algoritma dan panjang kunci perlu disertai mode operasi serta pengelolaan kunci yang tepat, sehingga efisiensi dan keamanan aplikasi tidak disimpulkan dari nama algoritma saja.

AES memproses blok berukuran 128 bit dengan pilihan panjang kunci 128, 192, atau 256 bit. Ketiganya menggunakan masing-masing 10, 12, dan 14 putaran transformasi (Roldán Lombardía dkk., 2021). Panjang kunci memperbesar ruang pencarian, sedangkan mode operasi mengatur hubungan antarblok. Dalam CBC, cipherteks blok sebelumnya terlibat dalam pemrosesan blok berikutnya. Pengujian CBC dengan ketiga panjang kunci pada Java, Node.js, PHP, dan Python menunjukkan pentingnya membedakan pilihan algoritma dari karakteristik implementasi platform (Arnaut dkk., 2021).

Berbagai penelitian terdahulu telah membahas penerapan Rijndael/AES dalam pengamanan data, sebagaimana dirangkum pada Tabel 1. Sianipar dkk. (2019) menerapkan Rijndael untuk pengamanan file suara, Yuliani dkk. (2019) mengombinasikan AES dengan steganografi, Siringoringo (2020) mengkombinasikan AES dan RSA, Nugrahantoro dkk. (2020) meneliti AES mode CBC, Putra dkk. (2020) mengimplementasikan AES pada aplikasi desktop, dan Bimantoro serta Sari (2021) mengamankan pesan instan mobile. Sintesis pada Tabel 1 memperlihatkan variasi objek dan metode yang dilaporkan. Tabel ini tidak merupakan penelaahan sistematis yang dapat memastikan kelengkapan evaluasi kuantitatif seluruh penelitian terdahulu.

Penelitian yang lebih dekat pada pengamanan dokumen digital dilakukan oleh Ananda dkk. (2022), yang mengimplementasikan aplikasi AES-128 untuk enkripsi dan dekripsi dokumen. Studi tersebut menjadi pembanding penerapan pada berkas, sedangkan penelitian ini mencakup dokumen, gambar, dan audio. Pada tingkat implementasi, Roldán Lombardía dkk. (2021) meneliti rangkaian AES-128/192/256 dengan pendekatan bit-serial. Perbedaan sasaran perangkat keras dan aplikasi desktop perlu diperhatikan sehingga hasil efisiensi rangkaian tidak digunakan sebagai hasil kinerja aplikasi ini.

Evaluasi enkripsi tidak cukup dijelaskan melalui keberhasilan pemulihan saja. Saraiva dkk. (2019) mengukur waktu eksekusi, throughput, dan konsumsi daya beberapa algoritma simetris, sedangkan Arnaut dkk. (2021) membandingkan biaya enkripsi/dekripsi AES-CBC pada platform web. Untuk objek citra, Gao dkk. (2022) menyajikan analisis korelasi, entropi, dan pengujian perubahan piksel melalui NPCR serta UACI pada skema berbasis chaos. Skema tersebut berbeda dari AES-CBC, tetapi memberi contoh pelaporan evaluasi citra yang terperinci. Nilai yang diperoleh pada penelitian-penelitian tersebut tidak dipindahkan menjadi hasil eksperimen penelitian ini.

Tabel 1. Ringkasan penelitian terdahulu dan posisi penelitian

No.	Peneliti dan tahun	Objek / Fokus	Metode	Hasil yang Dicapai
1	Sianipar dkk. (2019)	Pengamanan file suara	Rijndael	Enkripsi/dekripsi berhasil tanpa perubahan signifikan kualitas suara.
2	Yuliani dkk. (2019)	Keamanan file stego-object	AES	AES efektif mengamankan file yang disisipkan pada steganografi.
3	Fadlan dkk. (2019)	Pengamanan data teks	Beaufort & Caesar Cipher	Kombinasi algoritma klasik meningkatkan kompleksitas sandi teks.
4	Siringoringo (2020)	Pengamanan file umum	Rijndael (AES) & RSA	Kombinasi algoritma meningkatkan keamanan dibanding model tunggal.
5	Nugrahantoro dkk. (2020)	Optimasi keamanan informasi	AES CBC (128/192/256 bit)	Mode CBC meningkatkan ketahanan analisis pola dan frekuensi.
6	Putra dkk. (2020)	Aplikasi keamanan data	AES (Rijndael)	Rijndael terbukti andal untuk aplikasi keamanan data desktop.
7	Bimantoro & Sari (2021)	Instant messaging mobile	Kombinasi AES & RSA	Kombinasi AES-RSA mampu mengamankan teks dan gambar.
8	Batubara dkk. (2021)	Keamanan kata sandi	Algoritma BCRYPT	BCRYPT tahan terhadap serangan brute force.
9	Awal dkk. (2022)	Perbandingan hasil enkripsi	Rijndael & Twofish	Rijndael menunjukkan kualitas hasil enkripsi yang kompetitif.
10	Penelitian Ini	Pengamanan multi-file digital	Rijndael CBC 256 bit	Evaluasi ukuran tampil dan pemulihan fungsional; metrik kriptografis memerlukan validasi.

Penelitian ini bertujuan mengevaluasi fungsi enkripsi dan dekripsi pada aplikasi desktop Rijndael CBC 256 bit untuk berkas PDF, JPEG, dan MP3. Pertanyaan yang diperiksa adalah apakah berkas dapat dipulihkan untuk digunakan kembali dan apakah terdapat perbedaan ukuran pada ketelitian tampilan KB/MB yang dilaporkan. Kontribusinya adalah dokumentasi implementasi dan pengujian fungsional lintas format. Cakupan ini belum mencakup pembuktian kebaruan algoritma, benchmark antarvarian AES, atau pengujian ketahanan terhadap serangan.

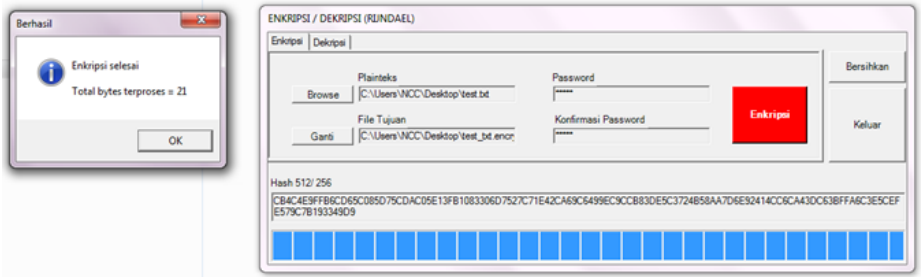
METODE PENELITIAN

Penelitian menggunakan pendekatan eksperimental untuk implementasi dan pengujian fungsional aplikasi. Tahapannya meliputi analisis kebutuhan, perancangan antarmuka, implementasi Rijndael CBC, serta pemeriksaan hasil enkripsi dan dekripsi. AES-256 menggunakan 14 putaran dengan transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey; MixColumns tidak diterapkan pada putaran terakhir

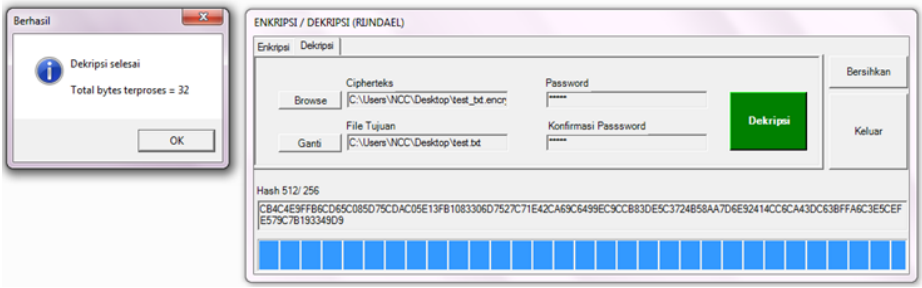
(Roldán Lombardía dkk., 2021). Pengujian berkas menggunakan kunci 256 bit, sedangkan variasi 128 dan 192 bit dibahas secara teoretis dalam Tabel 5.

Pada CBC, blok pertama dienkripsi setelah di-XOR dengan IV, sedangkan blok berikutnya di-XOR dengan cipherteks blok sebelumnya. IV perlu tersedia saat dekripsi dan harus dibangkitkan secara tepat untuk penggunaan CBC. Evaluasi CBC pada beberapa platform dan panjang kunci juga perlu memperhatikan perbedaan implementasi perangkat lunak (Arnaut dkk., 2021). Password pada antarmuka dibedakan dari kunci biner AES. Rincian pembangkitan dan penyimpanan IV, derivasi password menjadi kunci, serta padding belum terdokumentasi secara lengkap dalam penelitian ini. Oleh sebab itu, keamanan implementasi tidak disimpulkan hanya berdasarkan panjang kunci.

Aplikasi menyediakan antarmuka untuk memilih berkas, memasukkan serta mengonfirmasi password, dan menjalankan enkripsi atau dekripsi. Gambar 1 menunjukkan antarmuka enkripsi, sedangkan Gambar 2 menunjukkan antarmuka dekripsi. Keduanya digunakan untuk menjelaskan alur penggunaan aplikasi. Angka ukuran pada tangkapan layar tidak digunakan sebagai bukti kesamaan biner karena ukuran masukan dan keluaran harus dibandingkan pada tahap pemrosesan yang sama.



Gambar 1. Antarmuka sistem pada proses enkripsi berkas teks



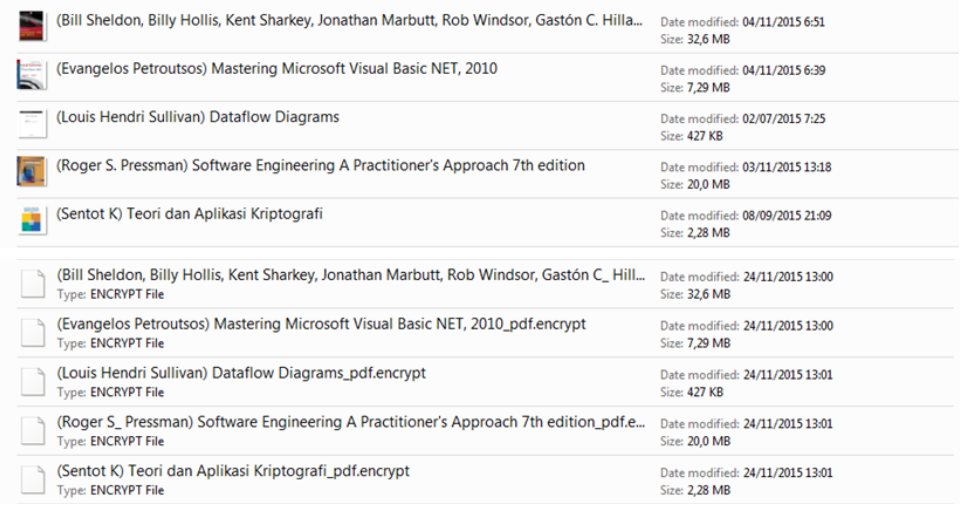
Gambar 2. Antarmuka sistem pada proses dekripsi berkas

Sampel pengujian terdiri atas 15 berkas: lima PDF, lima JPEG, dan lima MP3, sebagaimana dirinci dalam Tabel 2–4. Alur pengujian meliputi pemilihan berkas, enkripsi, pencatatan ukuran tampil plainteks dan cipherteks, dekripsi, serta pemeriksaan kemampuan membuka atau memutar hasil pemulihan. Ukuran tampil dipertahankan dalam satuan dan ketelitian yang tersedia pada dokumentasi pengujian; nilai tersebut tidak dikonversi menjadi ukuran byte eksak. Status pulih secara fungsional menunjukkan berkas hasil dekripsi dapat digunakan kembali. Status ini tidak menyatakan kesamaan byte atau hash. Pemilihan sampel, jumlah pengulangan, dan lingkungan eksekusi belum terdokumentasi

secara lengkap sehingga pengujian ini diperlakukan sebagai evaluasi deskriptif pada sampel yang tersedia.

DISKUSI DAN PEMBAHASAN

Pengamatan ukuran berkas dilakukan secara deskriptif, tanpa uji signifikansi statistik. Lima berkas PDF memiliki ukuran tampil antara 427 KB dan 32,6 MB. Gambar 3 memperlihatkan dokumentasi tampilan berkas, sedangkan Tabel 2 merangkum ukuran yang tercatat serta status pemulihan fungsional. Ukuran yang sama pada tampilan tidak diperlakukan sebagai bukti bahwa enkripsi tidak menambah byte.

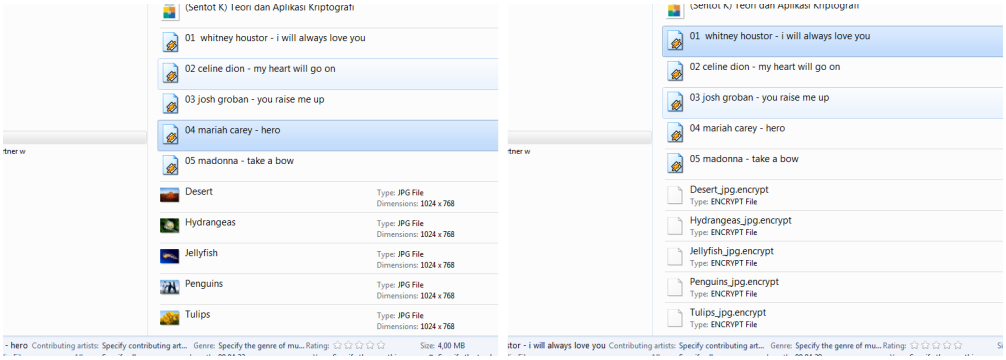


Gambar 3. Perbandingan ukuran tampil berkas dokumen PDF plainteks (atas) dan cipherteks (bawah)

Tabel 2. Ukuran tampil dan pemulihan fungsional berkas PDF

No.	Nama Berkas Dokumen (PDF)	Kapasitas Plainteks	Kapasitas Cipherteks	Perubahan ukuran tampil	Pemulihan fungsional
1	Bill Sheldon et al. - Professional VB	32,6 MB	32,6 MB	Tidak tampak pada pembulatan	Pulih secara fungsional
2	Evangelos Petroutsos - Mastering VB.NET	7,29 MB	7,29 MB	Tidak tampak pada pembulatan	Pulih secara fungsional
3	Louis Hendri Sullivan - Dataflow Diagrams	427 KB	427 KB	Tidak tampak pada pembulatan	Pulih secara fungsional
4	Roger S. Pressman - Software Engineering 7th	20,0 MB	20,0 MB	Tidak tampak pada pembulatan	Pulih secara fungsional
5	Sentot K. - Teori dan Aplikasi Kriptografi	2,28 MB	2,28 MB	Tidak tampak pada pembulatan	Pulih secara fungsional

Berdasarkan Tabel 2 dan Gambar 3, ukuran tampil dokumen PDF sama pada pembulatan KB/MB yang dilaporkan. Kesamaan tersebut belum membuktikan kesamaan jumlah byte. Pengujian berikutnya melaporkan lima berkas JPEG beresolusi 1024 × 768 piksel; perbandingan visual dan ukuran tampil disajikan pada Gambar 4 dan Tabel 3.

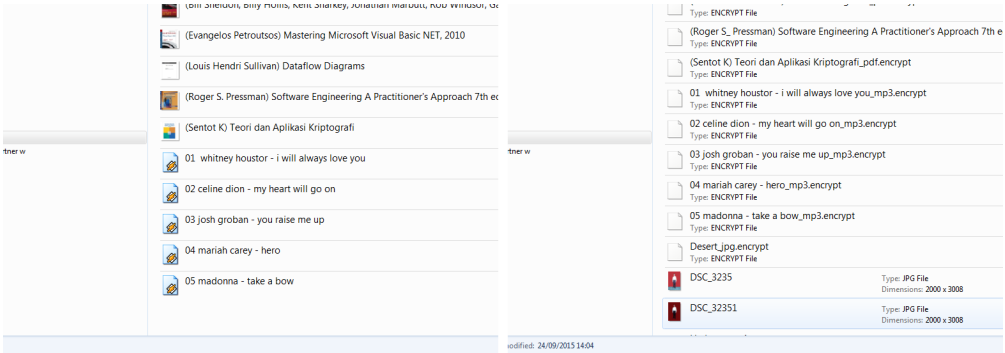


Gambar 4. Perbandingan tampilan berkas gambar JPEG plainteks (kiri) dan cipherteks (kanan)

Tabel 3. Ukuran tampil dan pemulihan fungsional berkas JPEG

No.	Nama Berkas Gambar (JPG)	Dimensi Spasial	Ukuran Plainteks	Ukuran Cipherteks	Pemulihan fungsional
1	Desert.jpg	1024 x 768 piksel	826 KB	826 KB	Pulih secara fungsional
2	Hydrangeas.jpg	1024 x 768 piksel	581 KB	581 KB	Pulih secara fungsional
3	Jellyfish.jpg	1024 x 768 piksel	757 KB	757 KB	Pulih secara fungsional
4	Penguins.jpg	1024 x 768 piksel	759 KB	759 KB	Pulih secara fungsional
5	Tulips.jpg	1024 x 768 piksel	606 KB	606 KB	Pulih secara fungsional

Tabel 3 melaporkan ukuran tampil yang sama sebelum dan sesudah enkripsi pada pembulatan yang digunakan. Pengujian berikutnya meliputi lima berkas MP3. Perbandingan berkas dan rekapitulasi ukuran tampil disajikan pada Gambar 5 dan Tabel 4.



Gambar 5. Perbandingan berkas audio MP3 plainteks (kiri) dan cipherteks (kanan)

Tabel 4. Ukuran tampil dan pemulihan fungsional berkas MP3

No.	Nama Berkas Audio (MP3)	Durasi Audio	Ukuran Plainteks	Ukuran Cipherteks	Pemulihan fungsional
1	01 whitney houston - i will always love you	04:29	4,11 MB	4,11 MB	Pulih secara fungsional
2	02 celine dion - my heart will go on	04:41	4,29 MB	4,29 MB	Pulih secara fungsional
3	03 josh groban - you raise me up	04:52	4,45 MB	4,45 MB	Pulih secara fungsional
4	04 mariah carey - hero	04:22	4,00 MB	4,00 MB	Pulih secara fungsional
5	05 madonna - take a bow	04:32	4,16 MB	4,16 MB	Pulih secara fungsional

Ukuran tampil pada Tabel 2–4 menunjukkan tidak adanya perubahan yang terlihat pada pembulatan KB/MB. Perbandingan ini harus dibedakan dari overhead byte aktual. Jika PKCS#7 diterapkan pada blok 16 byte, panjang cipherteks tanpa IV dan metadata adalah $C = 16 \times (\lfloor L/16 \rfloor + 1)$, dengan L sebagai panjang plainteks dalam byte. Dengan demikian, padding menambah 1–16 byte; ukuran IV dan metadata perlu dihitung terpisah. Persamaan ini merupakan penjelasan teoretis bersyarat, bukan pengukuran padding aplikasi. Tanpa ukuran byte aktual dan dokumentasi format keluaran, hasil yang dapat disimpulkan adalah kesamaan ukuran tampil, bukan overhead tepat 0%.

Berkas hasil dekripsi dapat dibuka atau diputar kembali menggunakan aplikasi sesuai formatnya. Oleh sebab itu, Tabel 2–4 menggunakan istilah pulih secara fungsional. Verifikasi biner memerlukan pembandingan byte atau digest sebelum enkripsi dan setelah dekripsi. Pemeriksaan tersebut berbeda dari autentikasi terhadap modifikasi oleh pihak lain. Zhang dkk. (2021) memadukan enkripsi AES dan autentikasi melalui GCM dalam sistem tertanam untuk menghadapi kebocoran dan manipulasi data. Hasil pada sistem tersebut menjadi contoh pemisahan tujuan kerahasiaan dan integritas, bukan bukti bahwa aplikasi CBC dalam penelitian ini telah menyediakan autentikasi.

Pengukuran MSE, PSNR, dan avalanche effect belum tersedia secara terperinci. Oleh karena itu, penelitian ini tidak melaporkan nilai metrik tersebut sebagai hasil eksperimen. Kemampuan membuka kembali berkas dan kesamaan ukuran tampil juga tidak digunakan sebagai pengganti pengukuran difusi, autentikasi, atau ketahanan terhadap serangan.

Tabel 5 menyajikan perbandingan teoretis AES berdasarkan panjang kunci dan jumlah putaran (Roldán Lombardía dkk., 2021). Ruang kandidat adalah 2^k untuk kunci k bit; nilai ini bukan waktu serangan yang terukur. Dengan asumsi kunci seragam dan urutan pencarian tanpa pengulangan, jumlah percobaan rata-rata mendekati 2^(k−1). Estimasi waktu masih memerlukan laju percobaan. Kinerja implementasi juga dipengaruhi platform: Saraiva dkk. (2019) mengevaluasi waktu eksekusi, throughput, dan konsumsi daya pada perangkat IoT. Oleh karena itu, urutan kecepatan AES-128, AES-192, dan AES-256 tidak ditetapkan sebagai hasil pengujian aplikasi ini tanpa benchmark yang sebanding.

Tabel 5. Karakteristik teoretis AES menurut panjang kunci

Panjang Kunci	Jumlah Putaran (Round)	Ruang Kunci (Kombinasi)	Interpretasi Ruang Kunci	Status Evaluasi Kinerja
128 bit	10 Putaran	2^128 (3,4 x 10^38)	Ruang pencarian teoretis 2^128	Belum diukur dalam naskah
192 bit	12 Putaran	2^192 (6,2 x 10^57)	Ruang pencarian teoretis 2^192	Belum diukur dalam naskah
256 bit	14 Putaran	2^256 (1,15 x 10^77)	Ruang pencarian teoretis 2^256	Belum diukur dalam naskah

Keterbatasan penelitian meliputi jumlah sampel yang terbatas, ketelitian ukuran berkas yang dibulatkan, serta belum tersedianya pembandingan biner, benchmark waktu, dan hasil difusi per sampel. Spesifikasi perangkat keras, versi library, prosedur pemilihan berkas, dan pengulangan belum tercatat secara lengkap sehingga reproduksibilitas belum dapat dinilai. Hasil fungsional karena itu tidak digeneralisasikan sebagai jaminan keamanan kriptografis pada seluruh kondisi.

KESIMPULAN

Rijndael CBC dengan kunci 256 bit berhasil diimplementasikan pada aplikasi desktop dan mendukung pemulihan fungsional terhadap 15 berkas yang diuji, terdiri atas PDF, JPEG, dan MP3. Ukuran tampil plainteks dan cipherteks tetap sama pada ketelitian KB/MB yang digunakan. Kesamaan tersebut belum menunjukkan overhead nol dalam byte ataupun kesamaan biner. Perbandingan panjang kunci memberikan penjelasan teoretis mengenai ruang pencarian, bukan hasil simulasi serangan. Kontribusi penelitian terletak pada implementasi dan evaluasi fungsional multi-format, dengan penilaian keamanan menyeluruh sebagai pekerjaan lanjutan.

Pengembangan berikutnya perlu mencatat ukuran aktual dalam byte, memverifikasi digest sebelum dan sesudah pemrosesan, serta menguji performa dan difusi dengan prosedur berulang. Pengelolaan IV dan derivasi kunci juga perlu didokumentasikan. Implementasi AES-GCM oleh Zhang dkk. (2021) memberikan contoh integrasi enkripsi dan autentikasi yang dapat dikaji sebagai arah pengembangan. Namun, hasil pada perangkat keras sistem tertanam tersebut tidak langsung disamakan dengan performa aplikasi desktop dalam penelitian ini.

UCAPAN TERIMA KASIH

Penelitian ini didanai oleh hibah Penelitian Dosen Institut Teknologi dan Kesehatan (ITEKes) Mahardika tahun pelaksanaan 2024. Penulis menyampaikan terima kasih yang sebesar-besarnya kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) ITEKes Mahardika atas dukungan pendanaan dan fasilitasi riset, serta kepada Program Studi Informatika Fakultas Teknik atas penyediaan sarana laboratorium komputasi.

KONTRIBUSI PENULIS

Para penulis menyatakan kontribusi mereka terhadap penelitian dan penyusunan naskah ini dalam format CRediT (Contributor Roles Taxonomy) sebagai berikut. Ade Sutriyono, S.Kom., M.MSI: Conceptualization, Methodology, Formal Analysis, Supervision, Project Administration, dan Writing - Original Draft; Dimas Dwi Rianto: Software, Validation, dan Investigation; Fasya Mahesa: Formal Analysis, Data Curation, dan Investigation; serta Indah Rizkika: Resources, Investigation, Data Curation, dan Writing - Review & Editing. Semua penulis telah membaca dan menyetujui versi akhir dari naskah ini.

PERNYATAAN KETERSEDIAAN DATA

Data sampel pengujian (dokumen, gambar, dan audio) beserta purwarupa kode program yang mendukung temuan dalam penelitian ini tersedia dari penulis korespondensi atas permintaan yang wajar.

PERNYATAAN BEBAS KONFLIK KEPENTINGAN

Para penulis menyatakan bahwa tidak ada konflik kepentingan finansial maupun hubungan personal yang dapat mempengaruhi keabsahan hasil penelitian yang dilaporkan dalam naskah ini.

PERNYATAAN ETIKA PENELITIAN DAN PUBLIKASI

Para penulis menyatakan bahwa penelitian dan penulisan naskah ini telah mematuhi prinsip etika penelitian ilmiah, orisinalitas karya, serta bebas dari plagiasi.

PERNYATAAN PEMANFAATAN TEKNOLOGI ASISTIF

Dalam penyiapan naskah, teknologi kecerdasan buatan generatif dan teknologi asistif digunakan untuk membantu penyuntingan bahasa, penerjemahan abstrak, penelusuran referensi, dan penajaman pembahasan berdasarkan hasil review. Penggunaan tersebut tidak mencakup pembuatan data atau hasil eksperimen. Penulis bertanggung jawab atas pemeriksaan sumber, keakuratan isi ilmiah, dan persetujuan versi akhir naskah.

REFERENSI

Ananda, S. P., Lukman, S., & Irfan. (2022). Analisa metode kriptografi modern Advance Encryption Standard (AES) 128 bit dalam mengenkripsi dan mendekripsi file dokumen digital. Jurnal Ilmiah Komputasi, 21(3), 333–344. https://doi.org/10.32409/jikstik.21.3.2973

Arnaut, U., Tair, M., & Veinović, M. (2021). Comparison of the efficiency of AES implementations on major web platforms. In Proceedings of the International Scientific Conference – Sinteza

2021 (pp. 153–157). Singidunum University. https://doi.org/10.15308/Sinteza-2021-153-157

Awal, E., Nurkifli, E. H., & Padilah, T. (2022). Analisis Perbandingan Hasil Enkripsi dan Dekripsi Algoritma Kriptografi Rijndael dan Twofish untuk Penyandian Data. Jurnal Mahasiswa Ilmu Komputer (JMIK), 3(1), 15–24.

Batubara, T. P., Efendi, S., & Nababan, E. B. (2021). Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force. Journal of Physics: Conference Series, 1811(1), 012129. https://doi.org/10.1088/1742-6596/1811/1/012129

Bimantoro, Y., & Sari, R. T. K. (2021). Enkripsi Data Menggunakan RSA dan AES pada Aplikasi Instant Messaging Berbasis Mobile. Jurnal Teknik Informatika, 14(2), 135–144. https://doi.org/10.15408/jti.v14i2.23469

Fadlan, M., Sinawati, S., Indriani, A., & Bintari, E. D. (2019). Pengamanan Data Teks Melalui Perpaduan Algoritma Beaufort dan Caesar Cipher. Jurnal Teknik Informatika, 12(2), 149–158. https://doi.org/10.15408/jti.v12i2.12262

Gao, X., Miao, M., & Chen, X. (2022). Multi-image encryption algorithm for 2D and 3D images based on chaotic system. Frontiers in Physics, 10, Article 901800. https://doi.org/10.3389/fphy.2022.901800

Nugrahantoro, A., Fadlil, A., & Riadi, I. (2020). Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Cipher Block Chaining (CBC). Jurnal Ilmiah FIFO, 12(1), 12–21. https://doi.org/10.22441/fifo.2020.v12i1.002

Putra, A. P., Maryana, S., & Setiawan, A. (2020). Implementasi Algoritma AES (Advance Encryption Standard) Rijndael pada Aplikasi Keamanan Data. JIPETIK: Jurnal Ilmiah Penelitian Teknologi Informasi dan Komputer, 6(2), 55–62.

Roldán Lombardía, S., Balli, F., & Banik, S. (2021). Six shades lighter: A bit-serial implementation of the AES family. Journal of Cryptographic Engineering, 11(4), 417–439. https://doi.org/10.1007/s13389-021-00265-8

Saraiva, D. A. F., Leithardt, V. R. Q., de Paula, D., Sales Mendes, A., González, G. V., & Crocker, P. (2019). PRISEC: Comparison of symmetric key algorithms for IoT devices. Sensors, 19(19), Article 4312. https://doi.org/10.3390/s19194312

Sianipar, K. D. R., Siahaan, S. W., Siregar, M., & Gunawan, I. (2019). Pengamanan File Suara Menggunakan Kriptografi Algoritma Rijndael dengan Proses Enkripsi dan Dekripsi. TECHSI - Jurnal Teknik Informatika, 11(3), 431–441. https://doi.org/10.29103/techsi.v11i3.1967

Siringoringo, R. (2020). Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File. KAKIFIKOM (Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer), 2(1), 31–42. https://doi.org/10.54367/kakifikom.v2i1.666

Yuliani, S. Y., Atmadja, A. R., Nurjanah, Y. S., Fauzy, D., Utomo, R. G., & Nur, D. R. (2019). Implementation of Advanced Encryption Standard for File Security in Stego-Object. Journal of Physics: Conference Series, 1402(6), 066095. https://doi.org/10.1088/1742-6596/1402/6/066095

Zhang, Z., Wang, X., Hao, Q., Xu, D., Zhang, J., Liu, J., & Ma, J. (2021). High-efficiency parallel cryptographic accelerator for real-time guaranteeing dynamic data security in embedded systems. Micromachines, 12(5), Article 560. https://doi.org/10.3390/mi12050560