5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

PENERAPAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* 256 (AES 256) BERBASIS *WEB* UNTUK MENGAMANKAN DOKUMEN PADA SELINDO TRAVEL

Christoforus Ade Kurniawan[1], Purwanto[2*]

[1,2] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Kota Tangerang, Indonesia

Email: [1]2011500358@student.budiluhur.ac.id, [2*]purwanto@budiluhur.ac.id
(* : corresponding author)

Abstrak- Keamanan data menjadi sangat penting di era modern, terutama bagi perusahaan perjalanan seperti Selindo Travel yang mengelola dokumen penting yang berisi data pribadi. Risiko kebocoran data dan akses tidak sah adalah masalah utama yang dihadapi. Untuk mengatasi masalah ini, penelitian ini menggunakan algoritma *Advanced Encryption Standard* (AES) 256-*bit* berbasis *web*. AES 256 dipilih karena memiliki tingkat keamanan yang tinggi dengan kunci enkripsi 256-*bit*. Penelitian ini menggunakan *ReactJS* untuk antarmuka pengguna dan *NodeJS* untuk pemrosesan data yang memungkinkan dokumen dienkripsi dan didekripsi dengan cepat tanpa menggunakan basis data atau *API* pihak ketiga. Metode *waterfall* digunakan untuk melakukan penelitian. Ini dimulai dengan perumusan masalah, penelitian literatur, perancangan sistem, implementasi, dan pengujian. Pengujian dilakukan dengan berbagai jenis *file* yang berbeda seperti *PDF*, gambar, *Word*, *Excel*, dan *CSV*. Hasil penelitian menunjukkan bahwa aplikasi dapat mengamankan dokumen sesuai dengan peraturan keamanan. Pengujian menunjukkan bahwa dokumen yang telah dienkripsi hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang benar, memenuhi aspek rahasia, kebenaran, dan aksesibilitas dalam keamanan data. Penelitian ini bertujuan untuk menyediakan solusi keamanan dokumen berbasis *web* yang efisien dan mudah digunakan yang dapat diintegrasikan dengan sistem Selindo Travel yang sudah ada. Diharapkan bahwa aplikasi yang menerapkan AES 256 ini dapat meningkatkan keamanan dan kepercayaan dalam pengelolaan dokumen digital di Selindo Travel.

Kata Kunci: Keamanan data, AES 256, ReactJS, NodeJS, Enkripsi.

Abstract- *Data security has become crucial in the modern era, especially for travel companies like Selindo Travel, which manages important documents containing personal data. The risks of data breaches and unauthorized access are the main issues faced. To address these problems, this research employs a web-based Advanced Encryption Standard (AES) 256-bit algorithm. AES 256 was chosen for its high level of security with a 256-bit encryption key. The study utilizes ReactJS for the user interface and NodeJS for data processing, allowing documents to be encrypted and decrypted quickly without the use of databases or third-party APIs. The waterfall method was used to conduct the research, starting with problem formulation, literature review, system design, implementation, and testing. Testing was conducted on various types of files, including PDFs, images, Word documents, Excel sheets, and CSV files. The results indicate that the application can secure documents in compliance with security regulations. Testing shows that encrypted documents can only be accessed by those with the correct decryption key, fulfilling the confidentiality, integrity, and availability aspects of data security. This research aims to provide an efficient and user-friendly web-based document security solution that can be integrated with Selindo Travel's existing systems. It is expected that the application implementing AES 256 could enhance security and trust in the management of digital documents at Selindo Travel.*

Keywords*: Data security, AES 256, ReactJS, NodeJS, Encryption..*

1. PENDAHULUAN

Dalam era digital saat ini, keamanan data sangat penting, terutama bagi bisnis perjalanan seperti Selindo Travel. Dokumen penting yang berisi data pelanggan, transaksi, dan informasi sensitif lainnya harus dilindungi dari kebocoran dan akses tidak sah. *Algoritma Advanced Encryption Standard* 256 (AES 256) merupakan salah satu teknik enkripsi yang dikenal secara luas karena kemampuan untuk menyediakan tingkat keamanan yang tinggi melalui penggunaan kunci enkripsi sepanjang 256 *bit*.

Selindo Travel menghadapi masalah dalam menjaga kerahasiaan dan integritas data mereka. Kebocoran data dapat merusak keuangan dan reputasi perusahaan. Oleh karena itu, sistem keamanan yang kuat diperlukan supaya data sensitif dapat terlindungi dari akses yang tidak sah. Sehingga, diperlukan solusi yang lebih canggih dan andal untuk melindungi data sensitif dari akses tidak sah.

Indonesia memiliki banyak penelitian tentang penggunaan algoritma kriptografi untuk keamanan data. AES telah digunakan untuk melindungi data pada sistem manajemen, aplikasi perbankan, dan aplikasi layanan

kesehatan. Beberapa penelitian telah menyelidiki penggunaan AES dalam berbagai konteks. Namun, sebagian besar penelitian ini berfokus pada implementasi di lingkungan yang tidak berbasis *web* atau menggunakan berbagai teknologi dan pendekatan, seperti *library* atau *API* pihak ketiga.

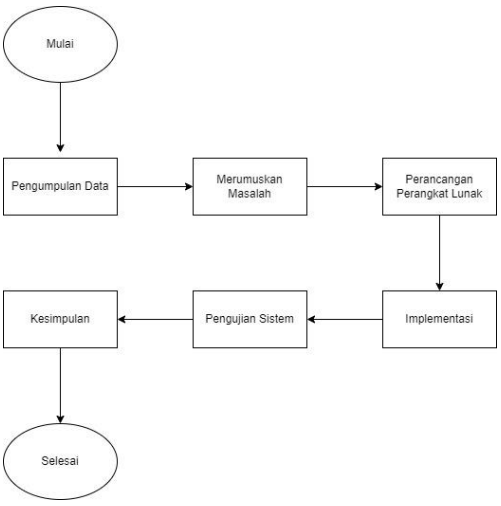
Penelitian ini berbeda dari penelitian sebelumnya yang berjudul ”Implementasi Algoritma AES Pada Aplikasi Pembelian *Voucher Hotspot* Berbasis *Android*” yang ditulis oleh [1] dikarenakan pada penelitian sebelumnya algoritma *Advanced Encryption Standard* (AES) diimplementasikan pada aplikasi berbasis *android* sedangkan pada penelitian ini algoritma AES diimplementasikan pada aplikasi berbasis *web* yang menawarkan keuntungan karena lebih mudah diakses dan dapat berkerja sama dengan sistem Selindo Travel yang sudah ada. Pada penelitian sebelumnya juga tidak membahas jenis algoritma AES apa yang digunakan sedangkan pada penelitian ini menggunakan algoritma AES-256 *bit* tanpa menggunakan *library* atau *API* kriptografi pihak ketiga sehingga metode ini memungkinkan kontrol penuh atas proses enkripsi dan dekripsi, meningkatkan keamanan sistem dan fleksibilitas.

Penelitian ini menyarankan Selindo Travel untuk membangun sistem keamanan dokumen berbasis *web* yang menggunakan algoritma AES-256. Sistem ini berperan untuk mengamankan dokumen *digital* dan memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi sensitif terkait. Solusi ini diharapkan dapat meningkatkan keamanan data dan dokumen penting di Selindo Travel, dengan enkripsi dokumen sebelum penyimpanan dan dekripsi saat akses, serta antarmuka yang mudah digunakan untuk pegawai Selindo Travel.

Dengan mengimplementasikan algoritma *Advanced Encryption Standard* (AES) 256 berbasis *web* tanpa bergantung pada *library* atau *API* kriptografi pihak ketiga, penelitian ini menawarkan fleksibilitas dan kontrol penuh atas proses enkripsi dan dekripsi dokumen. Selain itu, solusi yang ditawarkan dapat diintegrasikan langsung dengan sistem yang sudah ada di Selindo Travel, sehingga meningkatkan efisiensi operasional sambil melindungi data pribadi. Pengembangan aplikasi ini menunjukkan bagaimana teknologi *ReactJS* dan *NodeJS* dapat digunakan secara efektif dalam hal keamanan data, yang dapat menjadi referensi untuk pengembangan aplikasi serupa di industri lainnya. Selindo Travel terutama merasakan manfaat dari penelitian ini karena dapat melindungi lebih banyak data dan dokumen penting pelanggan dari kebocoran, yang dapat merusak reputasi dan kepercayaan pelanggan. Untuk industri teknologi informasi, penelitian ini memberikan contoh metode yang efektif dan efisien untuk menerapkan enkripsi data. Metode ini juga dapat digunakan oleh perusahaan lain yang memiliki kebutuhan serupa untuk menjaga dokumen digital mereka tetap aman. Studi ini juga menunjukkan bahwa teknologi modern seperti *ReactJS* dan *NodeJS* dapat digunakan untuk membuat aplikasi keamanan yang cepat, responsif, dan aman.

2. METODE PENELITIAN

Algoritma AES-256 digunakan untuk melakukan enkripsi dan dekripsi dokumen pada penelitian ini. Penelitian ini menggunakan metode *waterfall* yang memulai dengan merumuskan masalah penelitian dan melakukan studi literatur dengan membaca penelitian sebelum-sebelumnya. Cara kerja metode *waterfall* ini yaitu dengan menyelesaikan setiap tahapan yang ada lalu melanjutkan ke tahap berikutnya seperti yang terlihat pada gambar 1.



Gambar 1 Metode *Waterfall*

a. Pengumpulan Data: Pada tahap ini, peneliti mengumpulkan data dengan memembaca jurnal dan mempelajari teori-teori seperti kriptografi, cara mengamankan file, AES, dan lain-lainnya.
b. Merumuskan Masalah: Setelah data dikumpulkan, masalah dapat diidentifikasi dan dirumuskan dengan jelas supaya tujuan penelitian dan kebutuhan penelitian dapat diketahui.
c. Perancangan Perangkat Lunak: Berdasarkan perumusan masalah, desain sistem dan arsitektur perangkat lunak dibuat. Tahap ini mencakup perancangan teknis dan gambaran bagaimana perangkat lunak akan bekerja.
d. Implementasi: Pada tahap ini, gambaran yang telah dibuat diterjemahkan menjadi kode program yang dapat digunakan berdasarkan penelitian ini.
e. Pengujian Sistem: Setelah perangkat lunak dikembangkan, dilakukan pengujian untuk memastikan bahwa sistem berfungsi sesuai dengan spesifikasi yang ditentukan dan tidak terdapat kesalahan pada fungsi program.
f. Kesimpulan: Tahap akhir di mana hasil dari seluruh proses pengembangan dievaluasi, dan kesimpulan ditarik. Program dapat dikatakan selesai setelah perangkat lunak berfungsi dengan baik.

2.1 Tujuan Kriptografi

Ilmu kriptografi tidak hanya dibuat untuk menjaga keamanan pesan yang dikirimkan, tetapi juga memiliki tujuan bagi para pengguna [2]. Terdapat 5 tujuan kriptografi yaitu:

a. *Privacy* / *Confidentiality*: *Privacy* mengarah ke data yang rahasia [3] sedangkan *Confidentiality* lebih mengarah ke layanan yang digunakan untuk menjaga informasi dari siapapun kecuali yang memiliki kunci atau otoritas untuk membuka atau merubah informasi yang tersandi [4] .
b. *Integrity*: Memiliki arti bahwa informasi yang dikirim dan diterima dijamin bebas dari segala bentuk modifikasi yang dilakukan selain dari pengirim dan penerima [5].
c. *Authenticity*: Melakukan verifikasi identitas penerima dan pengirim sebelum melakukan pertukaran data [5].
d. *Availability*: Ketersediaan data dan informasi dalam suatu sistem komputer yang dapat dimanfaatkan oleh pihak yang memiliki akses [3].
e. *Access Control*: Pengaturan akses informasi yang berhubungan dengan klasifikasi data, privasi, dan mekanisme autentikasi [3].

2.2 Kriptografi Kunci Simetris

Salah satu jenis algoritma enkripsi yang dikenal adalah kriptografi kunci simetris yang menggunakan metode yang sama untuk melakukan enkripsi dan dekripsi, sehingga penggunaan kunci untuk melakukan kedua proses tersebut sama. Berbeda dengan kriptografi kunci asimetris, penggunaan kunci berbeda atau tidak sama untuk proses enkripsi dan dekripsi. Algoritma enkripsi kunci simetris masih digunakan hingga saat ini karena prosesnya yang cepat dan pengguna dapat dengan mudah mengingat kuncinya [6].

2.3 Advanced Encryption Standar (AES)

Dua kriptografer Belgia Vincent Rijmen dan John Daemen membuat algoritma enkripsi yang disebut Rijndael. Mereka dinyatakan sebagai pemenang dalam kompetisi algoritma enkripsi menggantikan *Data Encryption Standard* (DES) yang diselenggarakan di Amerika pada 26 November 2001 oleh *National Institute of Standards and Technology* (NIST). Karena keamanan enkripsi kriptografi lama, terutama DES (*Data Encryption Standard*), tidak lagi terjamin, standar enkripsi lanjutan AES dibuat untuk menggantikannya. Dikarenakan memungkinkan Anda menggunakan kunci rahasia yang sama untuk mengenkripsi data saat melakukan proses enkripsi, algoritma AES juga dikenal sebagai algoritma cipher blok simetris [7].

2.4 Algoritma Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma yang memperlukan kunci saat melakukan enkripsi ataupun dekripsi. Prosesnya dilakukan berkali-kali, yang disebut "putaran", dan jumlah putaran tergantung pada panjangnya kunci. Setiap putaran membutuhkan Ronde, yang masuk ke Ronde berikutnya. AES juga dapat melakukan enkripsi dan dekripsi data dengan panjang kunci yang berbeda, seperti 128 *bit*, 192 *bit*, dan 256 *bit*. Proses perulangan dalam enkripsi dapat juga disebut sebagai Ronde. Pada proses enkripsi di AES terdapat empat jenis konversi, yaitu [1]:

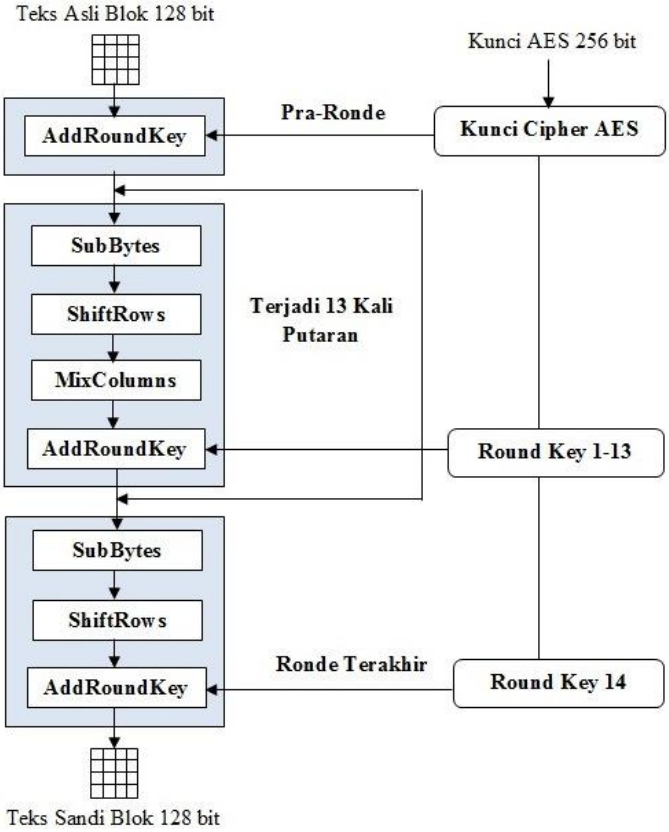
a. *SubBytes*: *SubBytes* memiliki prinsip untuk menukarkanan isi martiks atau tabel yang ada dengan matriks atau tabel lainnya yang disebut dengan *Rijndael S-Box* [8].
b. *ShiftRows*: sebuah proses yang melakukan pergeseran atau pergeseran pada setiap elemen blok atau tabel yang dilakukan pada setiap barisnya. Misalnya, baris pertama tidak melakukan pergeseran, baris kedua melakukan pergeseran satu byte, baris ketiga melakukan pergeseran dua byte, dan baris keempat melakukan pergeseran tiga byte [8].
c. *MixColumns*: *MixColumn* mengalikan tiap elemen dari blok *chiper* dengan matriks. Ini dilakukan dengan cara yang sama seperti perkalian matriks, menggunakan produk dot dan kemudian mengalikan keduanya ke dalam blok *chiper* baru [8].
d. *AddRoundKey*: Pada langkah ini, *chipertext* yang sudah ada digabungkan dengan *chiperkey* yang dihubungkan dengan XOR [7].

Sedangkan konversi pada proses deskripsi adalah [1]:

a. *InvShiftRow*
b. *InvSubBytes*
c. *InvMixColumn*
d. *AddRoundKey*

2.5 Proses Enkripsi AES

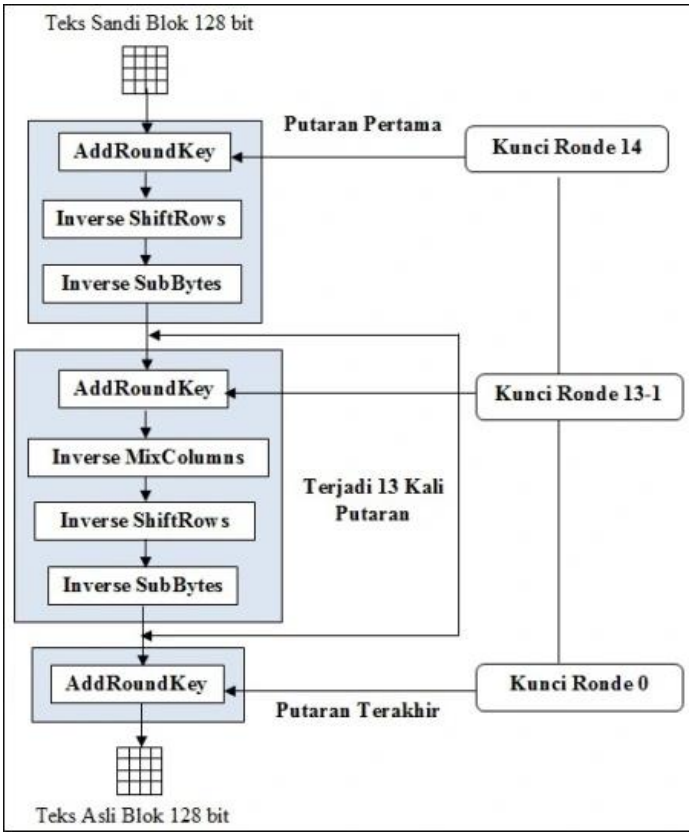
Pada awal proses, *input state* yang sudah disalin mengalami transformasi *AddRoundKey*. Kemudian, terdapat transformasi *state* menjadi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* yang diulang sebanyak Nr. Proses ini disebut *roundfunction* dalam algoritma AES. Dibandingkan dengan ronde sebelumnya, ronde terakhir tidak terdapat transformasi *MixColumns*. [9]. Berikut merupakan tahapan proses enkripsi yang juga dapat dilihat pada gambar 2.



Gambar 2 Tahapan Enkripsi

2.6 Proses Dekripsi AES

Ciphertext yang dibalik digunakan untuk mendekripsi AES. Untuk menghasilkan kata sandi terbalik, transformasi kriptografi menggunakan transformasi *byte InvSubBytes*, *InvShiftRows*, *InvMixColumns*, dan *AddRoundKey*. [10]. Berikut merupakan tahapan proses dekripsi yang juga dapat dilihat pada gambar 3.



Gambar 3 Tahapan Dekripsi

2.7 Keamanan Data

Keamanan data adalah usaha untuk menjaga kerahasiaan dan memastikan terpenuhinya tiga prinsip utama keamanan data. Prinsip-prinsip keamanan utama tersebut yaitu [11]:

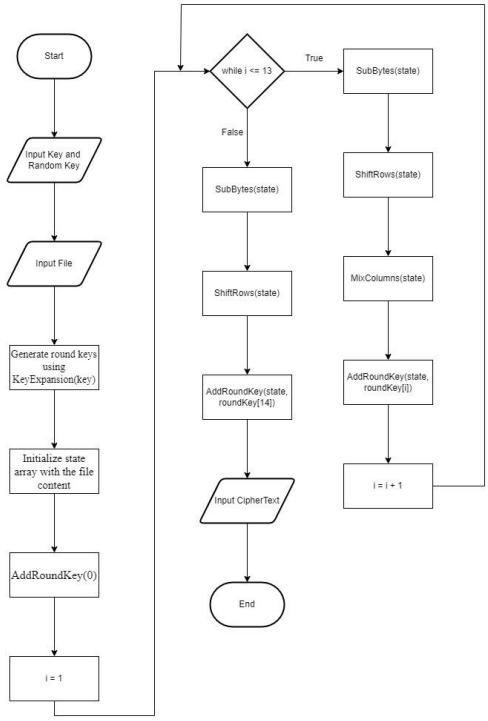
a. Kerahasiaan (*confidentiality*)
b. Integritas (*integrity*)
c. Ketersediaan (*availability*)

3. HASIL DAN PEMBAHASAN

Pada bagian ini *flowchart* tahapan enkripsi dan enkripsi, pengujian, dan tampilan layar diperlihatkan melalui gambar dan tabel.

3.1 Flowchart Tahapan Enkripsi

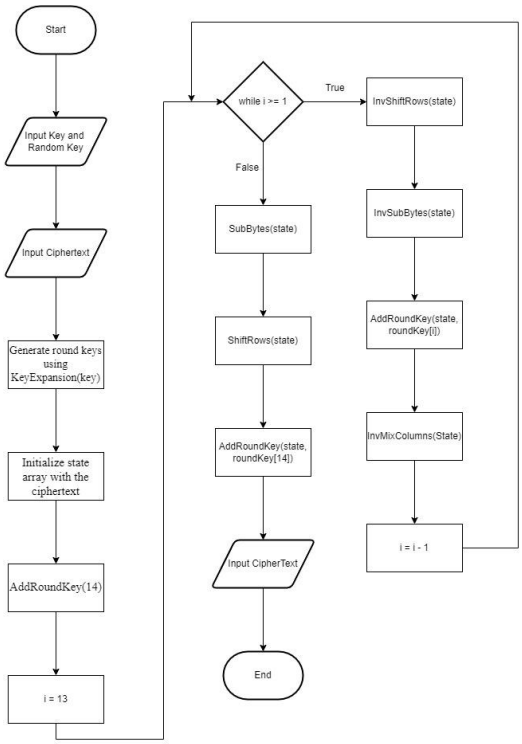
Flowchart dari tahapan enkripsi dapat dilihat pada gambar 4.



Gambar 4 *Flowchart* Tahapan Enkripsi

3.2 Flowchart Tahapan Dekripsi

Flowchart dari tahapan dekripsi dapat dilihat pada gambar 5.



Gambar 5 *Flowchart* Tahapan Dekripsi

3.3 Pengujian

Berikut merupakan hasil pengujian yang telah dilakukan menggunakan program ini. Pengujian enkripsi dapat dilihat pada tabel 1 dan pengujian dekripsi dapat dilihat pada tabel 2.

Tabel 1 Tabel Pengujian Enkripsi

No.	Nama File	Ukuran File	Nama File Enkripsi	Ukuran File Setelah Enkripsi	Durasi Enkripsi (detik)	Keterangan
1.	Resi Pak Edwin 09082022.pdf	205.49 KB	encrypted_Resi Pak Edwin 09082022.pdf	205.50 KB	0.26	Berhasil
2.	Resi Pak Edwin 09082022.docx	310.93 KB	encrypted_Resi Pak Edwin 09082022.docx	310.94 KB	0.40	Berhasil
3.	BDO.png	95.02 KB	encrypted_BDO.png	95.03 KB	0.12	Berhasil
4.	data enam bulan.xlsx	71.50 KB	encrypted_data enam bulan.xlsx	71.50 KB	0.09	Berhasil
5.	Data_Pelanggan_Apr2024.csv	174.93 KB	encrypted_Data_Pelanggan_Apr2024.csv	174.94 KB	0.21	Berhasil

Setelah dilakukan pengujian enkripsi pada beberapa *file* dengan format yang berbeda maka dapat dilihat bahwa beberapa *file* yang di proses ada yang memiliki perbedaan ukuran *file* serta ada yang sama juga dan semakin besar *file* yang di proses maka semakin lama proses enkripsi dilakukan.

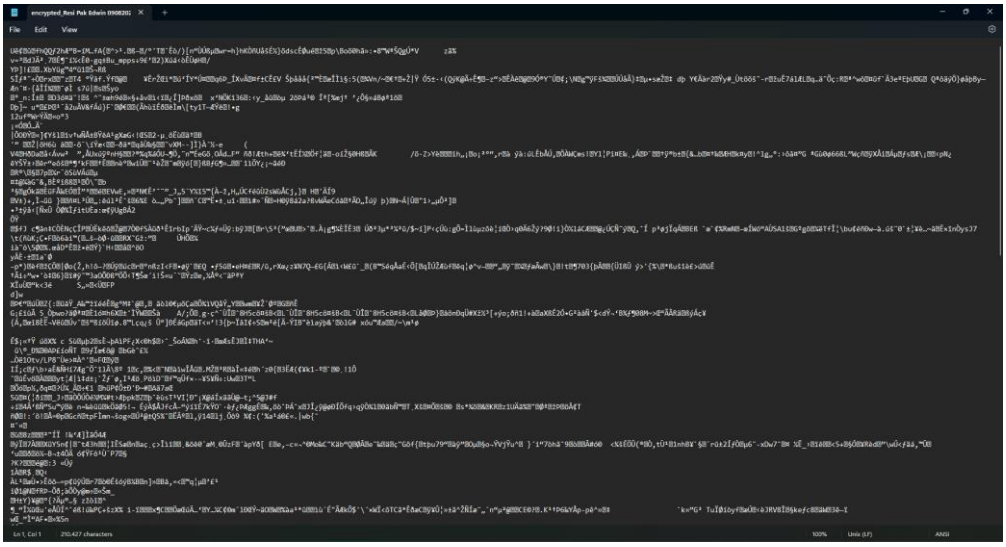
Tabel 2 Tabel Pengujian Dekripsi

No.	Nama File	Ukuran File	Nama File Dekripsi	Ukuran File Setelah Dekripsi	Durasi Dekripsi (detik)	Keterangan
1.	encrypted_Resi Pak Edwin 09082022.pdf	205.50 KB	decrypted_encrypted_Resi Pak Edwin 09082022.pdf	205.49 KB	0.41	Berhasil
2.	encrypted_Resi Pak Edwin 09082022.docx	310.94 KB	decrypted_encrypted_Resi Pak Edwin 09082022.docx	310.93 KB	0.62	Berhasil
3.	encrypted_BDO.png	95.03 KB	decrypted_encrypted_BDO.png	95.02 KB	0.20	Berhasil
4.	encrypted_data enam bulan.xlsx	71.50 KB	decrypted_encrypted_data enam bulan.xlsx	71.50 KB	0.13	Berhasil
5.	encrypted_Data_Pelanggan_Apr2024.csv	174.94 KB	decrypted_encrypted_Data_Pelanggan_Apr2024.csv	174.93 KB	0.33	Berhasil

Setelah dilakukan pengujian dekripsi pada beberapa *file* yang telah dienkripsi sebelumnya maka dapat dilihat bahwa ukuran *file* yang di proses kembali ke seperti ukuran awal file sebelum diproses enkripsi walaupun proses dekripsi memakan waktu yang lebih lama dari proses enkripsi.

3.4 Tampilan Dokumen Setelah Enkripsi

File yang telah dienkripsi memiliki format yang sama tetapi hanya tidak dapat dibuka dikarenakan telah dienkripsi tetapi jika peneliti ingin melihat hasil enkripsi maka peneliti dapat melakukan pengecekan dengan cara membuka *file* yang telah dienkripsi melalui program *Notepad*. Berikut tampilan *file* yang telah dienkripsi jika dibuka menggunakan program *Notepad* yang dapat dilihat pada gambar 6.



Gambar 6 Tampilan *File* di *Notepad*

4. KESIMPULAN

Penelitian ini menunjukkan bahwa aplikasi *web* yang menggunakan algoritma *Advanced Encryption Standard* (AES) 256 berhasil diterapkan untuk mengamankan *file* dalam berbagai format, seperti *PDF*, gambar, *Word*, *Excel*, dan *CSV*. Aplikasi yang dikembangkan menggunakan *ReactJS* dan *Material-UI* menunjukkan kinerja yang baik dalam proses enkripsi dan dekripsi, meskipun waktu yang dibutuhkan bervariasi tergantung pada ukuran *file*. Hasil analisis juga menunjukkan bahwa ukuran *file* setelah dienkripsi dapat tetap sama atau sedikit berbeda. Meskipun aplikasi ini tidak menggunakan basis data, yang membatasi pengelolaan *file* yang besar, antarmuka penggunanya yang ramah pengguna membuat mengunggah dan mengelola *file* lebih mudah. Untuk membuat keamanan data lebih terjaga dan tidak dapat diakses oleh pihak yang tidak berkepentingan, penelitian selanjutnya diharapkan dapat menggabungkan teknik kriptografi lainnya dalam pengamanan *file* dan menggunakan basis data sehingga pengelolaan *file* yang telah dienkripsi atau dekripsi dapat lebih mudah dilakukan.

DAFTAR PUSTAKA

[1] R. H. Irawan, U. Mahdiyah, and R. D. Kurniawan, ‘Implementasi Algoritma AES Pada Aplikasi Pembelian Voucher Hotspot Berbasis Android’, *Generation Journal*, vol. 8, no. 1, pp. 18–26, 2024, doi: 10.29407/gj.v8i1.20817.

[2] N. Wachid Hidayatulloh, M. Tahir, H. Amalia, N. Afdlolul Basyar, A. Faizal Prianggara, and M. Yasin, ‘Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data’, *Digital Transformation Technology (Digitech)*, vol. 03, no. no.1, pp. 1–10, 2023, [Online]. Available: https://jurnal.itscience.org/index.php/digitech/article/view/2293

[3] D. Widyawan and I. Imelda, ‘Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi’, *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.36080/skanika.v4i1.2216.

[4] S. D. Nurcahya, ‘Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java’, *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 5, no. 4, pp. 694–697, 2022, doi: 10.32672/jnkti.v5i4.4690.

[5] C. Irawan and E. H. Rachmawanto, ‘Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA’, *Proceeding SENDIU*, vol. l, no. 2, pp. 978–979, 2021.

[6] G. Y. P. Engko M, A. Id Hadiana, and P. Nurul Sabrina, ‘Kriptografi Untuk Enkripsi Ganda Pada Gambar Menggunakan Algoritma AES (Advanced Encryption Standard) Dan RC5 (Rivest Code 5)’, *Informatics and Digital Expert (INDEX)*, vol. 4, no. 1, pp. 25–32, 2022, doi: 10.36423/index.v4i1.884.

[7] N. M. S. Sianturi, N. B. Nugroho, and W. R. Maya, ‘Implementasi Kriptografi Untuk Pengamanan Data Aset Perusahaan Pada PT.PLN (Persero) Dengan Menggunakan Metode Algoritma AES 192’, *Jurnal CyberTech*, vol. 4, no. 1, pp. 44–59, 2020.

[8] M. Aria *et al.*, ‘Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Kota Medan dengan Menggunakan Algoritma AES’, *Journal on Education*, vol. 05, no. 03, pp. 6780–6787, 2023.

[9] B. E. Widodo, A. S. Purnomo, P. S. Informatika, F. T. Informasi, U. Mercu, and B. Yogyakarta, 'Implementasi Advanced Encryption Standard Pada Enkripsi Dan The Implementation Of Advanced Encryption Standard On The Encryption And Decryption Of The Confidential Documents At', vol. 1, no. 2, pp. 69–77, 2020.

[10] L. B. Handoko and C. Umam, 'Kombinasi Vigenere-Aes 256 dan Fungsi Hash Dalam Kriptografi Aplikasi Chatting', *Prosiding Sains Nasional dan Teknologi*, vol. 12, no. 1, p. 390, 2022, doi: 10.36499/psnst.v12i1.7068.

[11] R. Mulud Muchamad, A. Asriyanik, and A. Pambudi, 'Implementasi Algoritma Advanced Encryption Standard (Aes) Untuk Mengenkripsi Datastore Pada Aplikasi Berbasis Android', *Jurnal Mnemonic*, vol. 6, no. 1, pp. 55–64, 2023, doi: 10.36040/mnemonic.v6i1.5889.