3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI AES-128 UNTUK PENGAMANAN FILE BERBASIS WEB PADA PT. MARDIKA DAYA TRIBUANA

Abdul Haadziq Dartasanjaya[1], Dolly Virgian Shaka Yudha Sakti[2*]

[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta,

IndonesiaEmail: [1]haadziqa@gmail.com*, [2]dolly.virgianshaka@budiluhur.ac.id
(* : corresponding author)

Abstrak- Perkembangan teknologi informasi dan komunikasi saat ini membuat masyarakat dapat berkomunikasi dan bertukar informasi tanpa terhalang jarak dan waktu. Pentingnya pengamanan data pada perusahaan baik swasta maupun pemerintah untuk mencegah terjadinya tindak kejahatan seperti kebocoran informasi dan penyalahgunaan informasi oleh pihak yang tidak berwenang. PT MARDIKA DAYA TRIBUANA adalah perusahaan *corporate car rental* yang bergerak di bidang jasa pelayanan dalam penyewaan transportasi kepada perusahaan-perusahaan yang membutuhkan transportasi untuk keperluan hubungan kerja dan lain sebagainya. Perusahaan ini memiliki data yang cukup penting seperti data driver, data jenis dan tipe kendaraan, data sewa kendaraan, data perawatan komponen pada kendaraan, dan data transaksi keuangan yang masih disimpan dalam penyimpanan lokal komputer dan juga *flashdisk*. Hal ini tentu sangat berbahaya dan bisa membuat munculnya tindak kejahatan seperti pencurian data oleh pihak yang tidak bertanggungjawab. Untuk menjaga kerahasiaan dan keaslian data pada PT. MARDIKA DAYA TRIBUANA dibutuhkan suatu aplikasi dengan mengimplementasikan metode Kriptografi. Penelitian ini bertujuan untuk merancang aplikasi untuk membantu dalam proses pengamanan data. Teknik kriptografi yang digunakan adalah metode *Advanced Encryption Standard* (AES-128) yaitu dengan cara mengubah isi *file* dari yang bisa terbaca menjadi tidak terbaca (*encryption*) dan mengembalikan *file* kembali ke semula dan dapat terbaca kembali (*decryption*). Hasil yang diperoleh saat proses enkripsi dan dekripsi pada *file* adalah *file* tidak terjadi kerusakan sebelum dan sesudah di enkripsi maupun dekripsi.

Kata Kunci: Kriptografi, *Encryption*, *Decryption*, *File*, *Advanced Encryption Standard* (AES-128)

AES-128 IMPLEMENTATION FOR WEB-BASED FILE SECURITY AT PT. MARDIKA DAYA TRIBUANA

Abstract- *The current development of information and communication technology allows people to communicate and exchange information without being hindered by distance and time. The importance of securing data in companies, both private and government, is to prevent crimes such as information leakage and misuse of information by unauthorized parties. PT MARDIKA DAYA TRIBUANA is a corporate car rental company that operates in the field of transportation rental services to companies that need transportation for work relations and so on. This company has quite important data such as driver data, vehicle type and type data, vehicle rental data, vehicle component maintenance data, and financial transaction data which is still stored in the computer's local storage and flash drives. This is certainly very dangerous and can lead to crimes such as data theft by irresponsible parties. To maintain the confidentiality and authenticity of data at PT. MARDIKA DAYA TRIBUANA requires an application by implementing the Cryptographic method. This study aims to design applications to assist in the data security process. The cryptographic technique used is the Advanced Encryption Standard (AES-128) method, namely by changing the contents of the file from readable to unreadable (encryption) and returning the file back to its original state and can be read again (decryption). The results obtained during the encryption and decryption process on the file are that the file is not damaged before and after being encrypted or decrypted.*

Keywords*: Cryptography, Encryption, Decryption, Files, Advanced Encryption Standard (AES-128)*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini memungkinkan manusia untuk dapat berkomunikasi dan bertukar informasi tanpa terhalang jarak maupun waktu. Seiring meningkatnya kebutuhan keamanan kerahasiaan data yang dipertukarkan, hal ini meningkatkan kebutuhan akan tersedianya sistem keamanan informasi dan data yang lebih baik untuk melindungi data dari berbagai serangan[1]. Oleh karena itu,

pengembangan departemen yang mempelajari metode keamanan informasi berdampak positif pada persyaratan kegunaan sistem keamanan informasi yang melindungi data yang dikirim atau dikirim melalui jaringan komunikasi.

Hal ini tentunya akan berdampak besar dalam aspek kehidupan terutama dalam dunia bisnis, segala aspek kehidupan manusia dapat dengan mudah melakukan pertukaran data dalam berbagai bentuk tanpa batas ruang dan waktu[2]. Hal tersebut juga akan membuat peluang munculnya tindak kejahatan seperti bocornya informasi dan penyalahgunaan informasi oleh pihak yang tidak berwenang. Banyak sekali orang-orang melakukan kecurangan tanpa memikirkan dampak yang akan terjadi dimasa yang akan datang. Sehingga keamanan suatu informasi atau data menjadi sangat penting. Dalam kajian ini, peran teknologi sangat diperlukan dan salah satu peran teknologi adalah untuk menyimpan data, baik data yang bersifat umum maupun rahasia. Ilmu yang mempelajari tentang cara-cara pengamanan data dikenal dengan nama Kriptografi [3].

PT MARDIKA DAYA TRIBUANA adalah perusahaan *corporate car rental* yang bergerak di bidang jasa pelayanan dalam penyewaan transportasi kepada perusahaan-perusahaan yang membutuhkan transportasi untuk keperluan hubungan kerja dan lain sebagainya. PT MARDIKA DAYA TRIBUANA memiliki masalah pada data *file* seperti data driver, data kendaraan seperti jenis dan tipe kendaraan, data sewa kendaraan, data perawatan komponen pada kendaraan, dan juga data transaksi keuangan yang masih disimpan pada penyimpanan komputer dan tidak adanya pengamanan khusus untuk data-data tersebut. Karena bagi PT MARDIKA DAYA TRIBUANA data tersebut merupakan aset informasi yang berharga dan sangat rentan untuk terjadinya tindak kejahatan seperti pencurian data.

Pencurian data ini bisa saja disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Maka dari itu, perlunya pengimplementasian kriptografi *Advanced Encryption Standard* (AES-128) sebagai solusi dari permasalahan yang ada pada PT MARDIKA DAYA TRIBUANA untuk mengamankan serta melindungi data-data tersebut dari penyalahgunaan pihak yang tidak bertanggungjawab dengan menggunakan teknik enkripsi, sehingga data-data penting tetap bersifat rahasia dan tidak mudah untuk dimodifikasi. Kriptografi juga dapat menjadi solusi bagi perusahaan-perusahaan yang mempunyai data-data yang penting dan bersifat privasi untuk menyimpan data- data rahasia yang diperlukan pada kegiatan di masa mendatang nanti[4].

PT MARDIKA DAYA TRIBUANA ini masih banyak yang sistemnya masih berjalan seperti biasa, tanpa adanya peran dari teknologi. Contohnya pada proses penyimpanan data pelanggan atau pegawai yang hanya disimpan pada komputer tanpa adanya pengamanan kasus. Hal ini tentu sangat berbahaya dan bisa membuat tindak kejahatan seperti pencurian data dan lain sebagainya. Dalam menangani hal ini diperlukan teknik kriptografi yang bertujuan untuk melindungi dan mengamankan data dari penyalahgunaan pihak yang tidak bertanggung jawab[5].Berdasarkan uraian latar belakang penelitian tersebut yang telah dipaparkan diatas, pada penelitian ini maka aplikasi kriptografi dengan enkripsi algoritma AES dapat membantu dan menjaga kerahasiaan dan keaslian data pada PT MARDIKA DAYA TRIBUANA.

Pada penelitian ini dirancang dengan sebuah aplikasi kriptografi berbasis *web* menggunakan metode *Advanced Encryption Standard* (AES-128). Berdasarkan penelitian sebelumnya[5] membahas, AES dikenal sebagai algoritma yang memiliki kelebihan yakni, kemampuan dengan tingkat keamanan yang cukup tinggi. Pada penelitian sebelumnya metode yang digunakan adalah *Advanced Encryption Standard* (AES-256). Perbedaan dari AES-128 dengan AES-256 yaitu, AES-128 bit memiliki 10 putaran untuk enkripsi dan dekripsinya, sedangkan AES-256 memiliki 14 putaran. Karena Panjang kunci yang berbeda, ukuran blok yang akan diproses juga akan berpengaruh. Tentu saja ukuran blok juga bergantung pada panjang kunci. Dalam hal ini AES-128 memiliki perputaran lebih cepat dibandingkan dengan metode AES lainnya.

2. METODE PENELITIAN

Dalam melakukan penelitian terdapat beberapa rangkaian tahap yang dilakukan. Rangkaian tahap ini bertujuan untuk membuat penelitian menjadi terarah. Pada metode penelitian yang dilakukan saat ini menggunakan metode *waterfall*, dimulai dengan melakukan studi literatur dengan membaca hasil dari penelitian-penelitian terdahulu, kemudian melakukan studi lapangan dan dilanjutkan dengan perumusan masalah serta pengumpulan data, kemudian identifikasi permasalahan lalu analisis masalah dan dilanjutkan dengan perancangan perangkat lunak, berikutnya dilakukan implementasi serta pengujian pada sistem dan kesimpulan akhir sehingga diperoleh hasil dalam penelitian. Berikut ini adalah penjelasan dari setiap tahapan metode yang dilakukan dapat dilihat pada Gambar 1.

Gambar 1 Tahapan Penelitian

2.1 Studi Literatur

Studi literatur dilakukan dengan meninjau berbagai buku teks, jurnal, dan artikel ilmiah seputar penelitian yang dibahas, khususnya kriptografi dengan metode *Advanced Encryption Standard* (AES-128).

2.2 Studi Lapangan

Pada tahap ini dilakukan pengamatan langsung pada *file-file* penting di PT MARDIKA DAYA TRIBUANA.

2.3 Perumusan Masalah

Pada tahap ini terdapat isu ditemukan yang kemudian akan dibahas dan diselesaikan dalam penelitian ini, yaitu mengamankan data penyewaan kendaraan, pembelian dan penjualan kendaraan mobil, serta data laporan keuangan yang berada pada PT MARDIKA DAYA TRIBUANA dengan menerapkan algoritma dari kriptografi *Advanced Encryption Standard* (AES-128).

2.4 Pengumpulan Data

Pada tahap pengumpulan data ini terbagi menjadi 3 bagian, pertama melakukan observasi yaitu dengan mengamati dan mengetahui keadaan objek yang sebenarnya pada PT MARDIKA DAYA TRIBUANA. Kedua, melakukan wawancara dengan pihak yang berhubungan langsung dalam pembuatan perancangan aplikasi ini. Ketiga, studi kepustakaan yaitu dengan cara membaca *journal* atau *e-book* serta referensi yang ada kaitannya dengan metode kriptografi, teori keamanan *file*, teori *Advanced Encryption standard* (AES-128).

2.5 Identifikasi Permasalahan

Pada tahap ini setelah data-data sudah terkumpul langkah selanjutnya adalah membedah masalah yang ada pada sistem yang akan dibuat berdasarkan kendala yang ada. Dalam melakukan pembedahan permasalahan ini terbagi menjadi 3 tahapan, yaitu :

a. Analisis Data
b. Analisis Penerapan Algoritma
c. Analisis Sistem

2.6 Analisis Masalah

Pada tahap ini dilakukan persiapan apa saja untuk kebutuhan aplikasi pengamanan *file* dengan *algoritma* kriptografi metode *Advanced Encryption Standard* (AES-128).

2.7 Perancangan Perangkat Lunak

Pada tahap ini akan dilakukan perencanaan berdasarkan hasil analisis sistem, seperti perancangan modul enkripsi dan dekripsi yang akan dilakukan pada *file* serta komponen pendukung lainnya yang nantinya akan diimplementasikan kedalam aplikasi berbasis *web*, serta perancangan antarmuka pengguna.

2.8 Implementasi

Pada tahap ini modul-modul yang akan dirancang pada tahap desain akan dibuat menggunakan bahasa pemrograman tertentu. Dalam hal ini aplikasi yang digunakan yaitu :

1. *Software* yang digunakan untuk perancangan sistem pengamanan *file* berbasis *web* menggunakan bahasa pemrograman PHP dan Database yang digunakan adalah PHP My Admin.
2. *Hardware* yang digunakan yaitu Prosesor Intel Core i5, RAM 4GB DDR4, 500 GB HDD

2.9 Pengujian Sistem

Tahap ini akan dilakukan pengujian agar mengetahui sistem yang dibuat apakah sudah sesuai dengan analisis serta apakah aplikasi berbasis *web* ini sudah sesuai dengan yang diharapkan.

2.10 Kesimpulan Akhir

Proses ini adalah tahapan terakhir yaitu menarik kesimpulan akhir dari pengimplementasian metode enkripsi-dekripsi *Advanced Encryption Standard* (AES-128) dalam menjaga kerahasiaan serta keaslian *file* pada PT MARDIKA DAYA TRIBUANA sudah berfungsi dengan baik dan benar.

2.11 *Advanced Encryption Standard* (AES-128)

Advanced Encryption Standard (AES-128) adalah standar enkripsi kunci simetris yang diadopsi oleh pemerintah Amerika Serikat[6]. Standar tersebut mencakup atas 3 blok *cipher*, yaitu AES-128, AES-192 dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya dirilis sebagai Rijndael[7]. Setiap *cipher ber*ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit[8]. Algoritma AES merupakan block ciphertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi adalah mengubah data menjadi tidak terbaca ini disebut ciphertext, sebaliknya dekripsi adalah mengubah data ciphertext ke bentuk aslinya yang sering kita sebut sebagai plaintext[9]. Seseorang yang berusaha untuk mengembangkan dan membuat kode kriptografi *cryptographer* sedangkan untuk memecahkan kode disebut *cryptonalisis*[10]. Perbedaan type AES dapat dilihat pada tabel 1 dibawah ini:

Tabel 1 Jenis - jenis AES

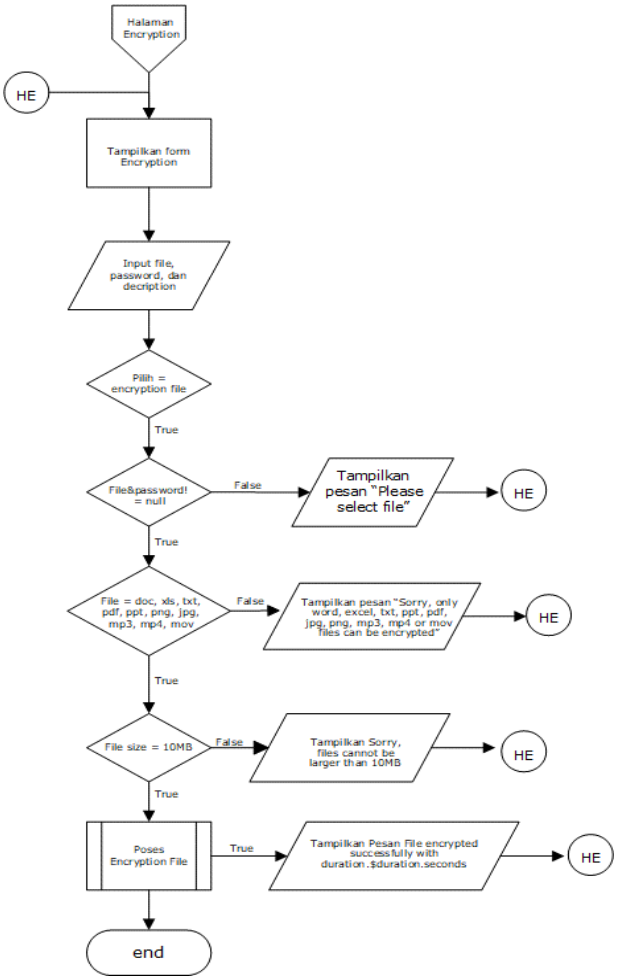
Jenis AES	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	128 Bit	128 Bit	10
AES-192	192 Bit	128 Bit	12
AES-256	256 Bit	128 Bit	14

3. HASIL DAN PEMBAHASAN

Pada tahapan ini akan dilakukan pengujian sistematik yang meliputi analisis, unjuk kerja atau hasil pengujian serta pembahasan topik penelitian, yang mungkin dilakukan sebelum metode penelitian. Bagian ini juga menyajikan penjelasan berupa penjelasan, gambar, tabel, dan lain-lain.

3.1 Flowchart Menu *File* Enkripsi

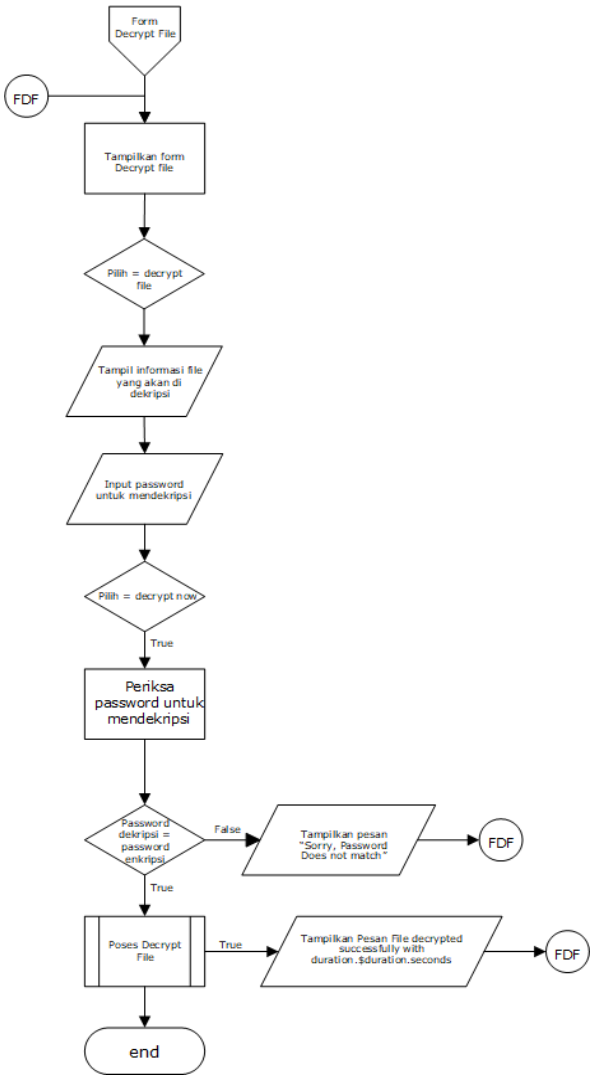
Pada bagian ini merupakan suatu proses untuk menjalankan menu *file* enkripsi. Berikut adalah flowchart pada rancangan menu *file* dapat dilihat pada gambar 2



Gambar 2 Flowchart Menu File Enkripsi

3.2 Flowchart Menu *File* Dekripsi

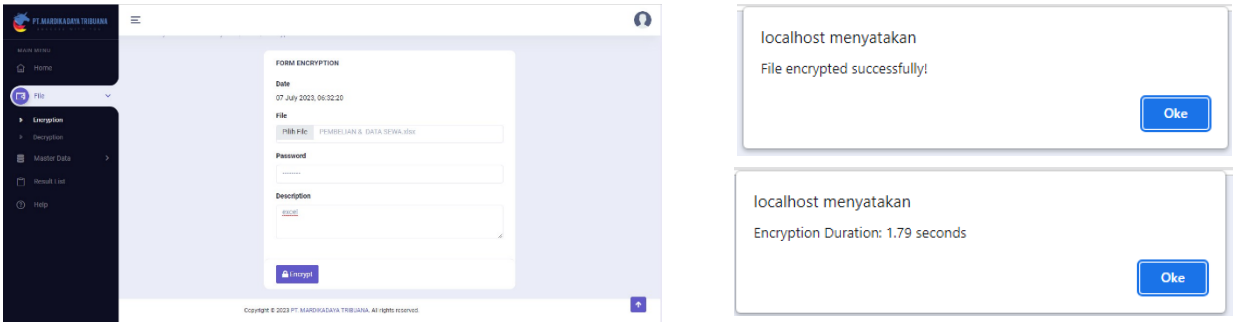
Pada bagian ini merupakan suatu proses untuk menjalankan menu *file* enkripsi. Berikut adalah flowchart pada rancangan menu *file* dapat dilihat pada gambar 3



Gambar 3 Flowchart Menu File Dekripsi

3.3 Proses *Encryption*

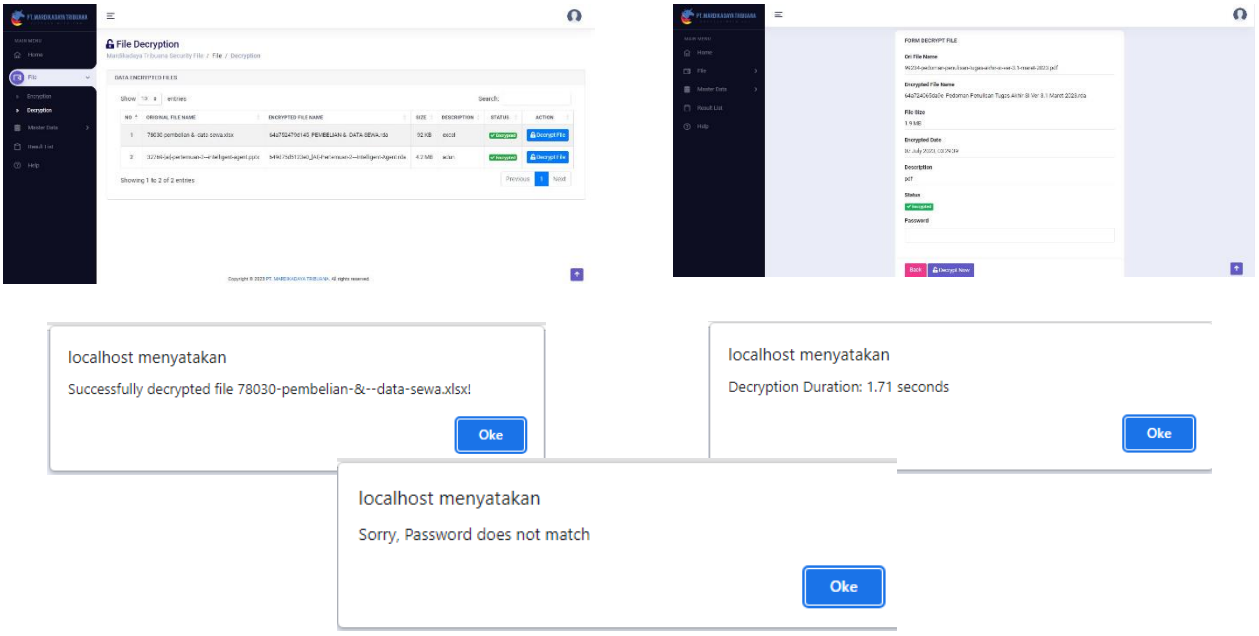
Pada bagian ini merupakan proses enkripsi *file* dengan cara menginput password agar *file* tidak dapat diakses oleh pihak lain. Berikut adalah proses enkripsi *file* dapat dilihat pada gambar 4



Gambar 4 Proses *Encryption*

3.4 Proses *Decryption*

Pada bagian ini meripakan proses dekripsi *file* dengan cara menginput password yang sudah dibuat pada proses pengenkripsian *file*. Berikut adalah proses dekripsi *file* dapat dilihat pada gambar 5



Gambar 5 Proses Decryption

3.5 Hasil Pengujian

Pada tahap ini merupakan tabel yang berisi dari hasil uji enkripsi dan dekripsi *file* yang dilakukan oleh sistem menggunakan aplikasi. Berikut adalah tabel hasil pengujian *file* seperti ditampilkan pada tabel dibawah ini.

Tabel 2 Tabel Hasil Uji *File* Enkripsi

No.	Nama *File* Awal	Ukuran *File* Awal	Nama *File* Enkripsi	Ukuran *File* Setelah Dienkripsi	Durasi Enkripsi	Keterangan
1	Studi Literatur.docx	26,4 KB	64a7701cc74b7_Sstudi-Literatur.rda	26,4 KB	0.49 seconds	BERHASIL
2	show password.txt	385 B	64a76fe05ac98_show-password.rda	385 B	0.01 seconds	BERHASIL
3	scytale.jpg	15,3 KB	64a76e6f2616b_scytale.rda	15,3 KB	0.36 seconds	BERHASIL
4	Picture 1155.mov	1,6 MB	64a76ee333d7e_Picture-1155.rda	1,6 MB	28.61 seconds	BERHASIL
5	PANDUAN-TOPIK-TUGASAKHIR-TI-Genap2023-	594,8 KB	64a76e1ef1a78_PANDUAN-TOPIK-TUGASAKHIR-TI-Genap2023-2024-v2-1.rda	594,8 KB	10.66 seconds	BERHASIL

No.	Nama *File* Awal	Ukuran *File* Awal	Nama *File* Enkripsi	Ukuran *File* Setelah Dienkripsi	Durasi Enkripsi	Keterangan
	2024-v2-1.pdf					
6	logo.png	7.8 KB	64a76e4da1a2b_logo.rda	7.8 KB	0.16 seconds	BERHASIL
7	PEMBELIAN & DATA SEWA.xlsx	92 KB	64a752479d145_PEMBELIAN-&--DATA-SEWA.rda	92 KB	1.79 seconds	BERHASIL

Tabel 3 Tabel Hasil Uji *File* Dekripsi

No.	Nama *File* Awal	Ukuran *File* Awal	Nama *File* Dekripsi	Ukuran *File* Dekripsi	Durasi Dekripsi	Keteranga n
1	Studi Litelatur.docx	26,4 KB	60935-studi-litelatur.docx	26,4 KB	0.5 seconds	BERHASIL
2	show password.txt	385 B	14545-show-password.txt	385 B	0.01 seconds	BERHASIL
3	scytale.jpg	15,3 KB	59199-scytale.jpg	15,3 KB	0.3 seconds	BERHASIL
4	Picture 1155.mov	1,6 MB	62819-picture-1155.mov	1,6 MB	29.41 seconds	BERHASIL
5	PANDUAN- TOPIK-TUGASAKHIR-TI-Genap2023-2024-v2-1.pdf	594,8 KB	51727-panduan- topik-tugasakhir-ti-genap2023-2024-v2-1.pdf	594,8 KB	11.25 seconds	BERHASIL
6	logo.png	7.8 KB	18605-logo.png	7.8 KB	0.16 seconds	BERHASIL
7	PEMBELIAN & DATA SEWA.xlsx	92 KB	78030-PEMBELIA N-&--DATA-SEWA.xlsx	92 KB	1.71 seconds	BERHASIL

4. KESIMPULAN

Setelah melakukan penelitian untuk mengamankan *file* pada PT Mardika daya Tribuana dengan metode kriptografi *Advanced Encryption Standard* (AES-128) berbasis *web*. Dapat disimpulkan bahwa dengan adanya sistem perancangan aplikasi yang dibuat dapat menjaga kerahasiaan dan keaslian data pada PT Mardika daya Tribuana. Tetapi juga, semakin besar ukuran *file* terenkripsi, semakin lama waktu yang dibutuhkan. Aplikasi ini didukung dengan format *file office* dengan ekstensi *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.txt dan *.pdf, serta mendukung format file gambar dengan ekstensi *.jpg, *.png, dan juga mendukung format audio dan video dengan ekstensi MP3, MP4 dan MOV. Diperlukan dilakukan penelitian lebih agar waktu dalam proses baik enkripsi maupun dekripsi dapat ditingkatkan lagi sekalipun *file* berukuran besar. Metode dapat dikembangkan dengan mengkombinasikan 2 hingga 3 metode kriptografi untuk meningkatkan keamanan secara maksimal.

DAFTAR PUSTAKA

[1] Y. Fatma, A. Hafid, and H. O. Dani, "Peningkatan Keamanan Pengiriman Pesan Teks: Kombinasi Advanced Encryption Standard (AES) 128 dan Least Significant Bit (LSB)," *JUSIFO (Jurnal Sist. Informasi)*, vol. 6, no. 2, pp. 111–120, 2020.

[2] H. Wijaya, "Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection," *Akad. J.*, vol. 17, no. 1, pp. 8–13, 2020.

[3] A. Z. F. Rangkuti and H. Fahmi, "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.

[4] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Skanika*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.36080/skanika.v4i1.2216.

[5] I. Kurnia Nurhareza and S. Siswanto, "PENERAPAN ALGORITMA KRIPTOGRAFI AES 256 UNTUK MENGAMANKAN DOKUMEN BERBASIS WEB PADA KELURAHAN BELENDUNG," 2022.

[6] Yusfrizal, "RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, 2019.

[7] R. Nuari, N. Ratama, J. T. Informatika, F. Teknik, and U. Pamulang, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 37–44, 2020.

[8] A. Widarma, H. F. Siregar, and M. D. Irawan, "Teknik Keamanan Data Menggunakan Vigenere Cipher Dan Electronic Code Book (ECB)," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 3, no. 2, p. 393, 2019, doi: 10.30645/j-sakti.v3i2.157.

[9] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[10] D. A. Sitepu, "Implementasi pengamanan data menggunakan algoritma Advanced Encryption Standart (AES)," *J. Ilm. Kaputama*, vol. 6, no. 1, pp. 49–58, 2022.