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

PENGAMANAN FILE BERBASIS WEB DENGAN MENERAPKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128)

Fariz Syaropal Anam[1], Titin Fatimah[2*]

[1,2*]Teknik Informatika, Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: [1]fariz.syaropal@gmail.com, [2*]titinfatimah@budiluhur.ac.id
(* : corresponding author)

Abstrak-CV Mitra Kurir Express adalah sebuah perusahaan yang bergerak di bidang logistik atau jasa pengiriman barang. Perusahaan ini memiliki data penting salah satunya yaitu data pengiriman barang. Pada perkembangan kemajuan teknologi saat ini, terutama dalam sistem keamanan data, telah mengalami perkembangan pesat. Keamanan data menjadi sangat penting dalam menjaga kerahasiaan informasi sensitif yang hanya boleh diakses oleh pihak yang berwenang. Oleh karena itu dibutuhkan aplikasi keamanan data berbasis web dengan menggunakan teknik kriptografi. Pada aplikasi kriptografi ini terdapat proses enkripsi dan dekripsi yang dapat mengamankan isi file berbentuk excel dan pdf. Pada penelitian ini dirancang sebuah sistem aplikasi kriptografi berbasis web menggunakan algoritma Advanced Encryption Standard (AES-128). Manfaat dari penelitian ini yaitu dapat melindungi data pengiriman barang dengan aman dan tidak perlu khawatir atas kebocoran data maupun pencurian data oleh pihak yang tidak berwenang. Hasil akhir pengujian rata-rata waktu yang dibutuhkan untuk proses enkripsi file yaitu 40.955 milidetik dan rata-rata waktu yang dibutuhkan untuk proses dekripsi file yaitu 6.295 milidetik.

Kata Kunci: Kriptografi, AES-128, File, Enkripsi, Dekripsi

WEB-BASED FILE SECURITY USING ADVANCED ENCRYPTION STANDARD (AES-128) ALGORITHM ON CV MITRA KURIR EXPRESS

Abstract-*CV Mitra Kurir Express is a company engaged in logistics or goods delivery services. This company has important data, one of which is goods delivery data. In the development of current technological advances, especially in data security systems, has experienced rapid development. Data security is very important in maintaining the confidentiality of sensitive information that can only be accessed by authorized parties. Therefore a web-based data security application is needed using cryptographic techniques. In this cryptographic application, there is an encryption and decryption process that can secure the contents of excel and pdf files. In this study a web-based cryptographic application system was designed using the Advanced Encryption Standard (AES-128) algorithm. So that with this application you can protect goods delivery data safely and you don't have to worry about data leakage or data theft by unauthorized parties.*

Keywords*: Cryptography, AES-128, File, encryption, Decryption*

1. PENDAHULUAN

Perkembangan teknologi yang semakin pesat setiap harinya telah membuat data atau informasi menjadi tak terpisahkan dari berbagai aspek kehidupan manusia. Tingkat pentingnya informasi pada setiap aspek tersebut dapat menyebabkan permasalahan dalam hal keamanan data atau informasi. Salah satu permasalahannya adalah upaya pencurian yang dilakukan oleh pihak ketiga atau pihak yang tidak bertanggung jawab terhadap data atau informasi yang akan kita kirim [1]. Seiring meningkatnya permintaan untuk menjaga kerahasiaan informasi yang dipertukarkan, kebutuhan akan ketersediaan data dan sistem keamanan informasi yang lebih baik semakin meningkat. Tujuannya adalah untuk melindungi data dari ancaman pencurian data [2]. Penelitian ini bertujuan untuk mengamankan file penting dari penyalahgunaan oleh pihak yang tidak berwenang

CV Mitra Kurir Express adalah perusahaan logistik atau jasa pengiriman barang. Meskipun saat ini era teknologi yang maju, perusahaan ini masih menggunakan prosedur manual dan semi komputerisasi. Data manual mencakup data pengiriman seperti nomor resi, nama pelanggan, alamat tujuan, nomor telepon, dan lain-lain. Sedangkan data semi komputerisasi diinput dan di output menggunakan aplikasi Ms. Office Excel. Dengan adanya dampak negatif dari perkembangan teknologi maka keamanan data dalam penyimpanan file atau data menjadi sangat penting [3]. Oleh karena itu, dibutuhkan teknik untuk mengamankan file tersebut yaitu menggunakan kriptografi.

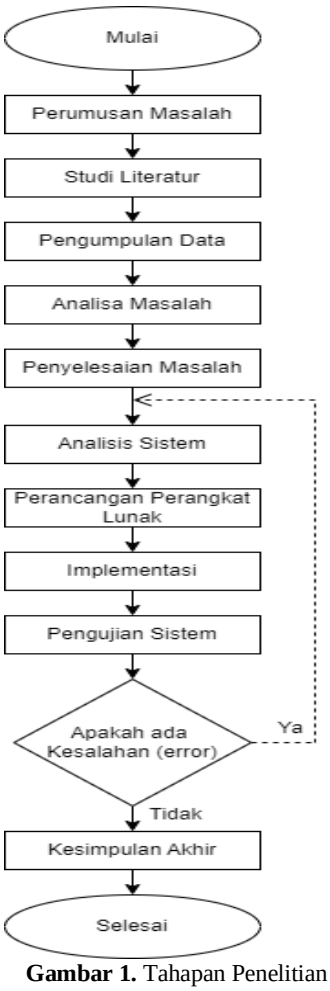
Kriptografi adalah bidang keahlian atau ilmu yang berkaitan dengan menyandikan atau mengamankan data atau informasi, termasuk aspek integritas data, kerahasiaan data, autentikasi data, dan data-data pribadi lainnya,

sehingga tidak dapat diakses oleh pihak yang tidak berhak [4]. Kriptografi berfungsi untuk menjaga keamanan pesan yang dikirimkan dari satu tempat ke tempat lain. Dengan menggunakan teknik kriptografi, pesan asli (plaintext) diubah atau dienkripsi menggunakan suatu kunci menjadi informasi acak yang tidak bermakna (ciphertext) [5]. Dalam bidang kriptografi terdapat berbagai algoritma, dan salah satunya adalah algoritma AES (*Advanced Encryption Standard*). Algoritma AES menggunakan panjang blok sebesar 128 bit dan mendukung panjang kunci sebesar 128, 192, dan 256 bit. Algoritma ini digunakan untuk mengenkripsi dan mendekripsi informasi dengan menggunakan proses berulang yang disebut ronde. Kelebihan AES adalah efisiensi biaya dan kemampuan untuk diimplementasikan dengan mudah pada memori berukuran kecil [6].

Pada penelitian sebelumnya yang berjudul "Implementasi Enkripsi dalam Pengamanan File Data Karyawan dengan Metode Algoritma DES (*Data Encryption Standard*) pada CV Sinergi Informasi Global". Pada penelitian tersebut, Sabar Hana dwi putra merancang sebuah aplikasi kriptografi untuk mengamankan file data karyawan menggunakan metode algoritma DES, yang dimana algoritma DES mengenkripsikan 64 bit plaintext menjadi 64 bit ciphertext dengan menggunakan 56 bit kunci internal [7]. Dan pada penelitian ini akan dirancang sebuah sistem pengamanan file berbasis web menggunakan metode AES-128 pada CV Mita Kurir Express.

2. METODE PENELITIAN

Tahap ini berperan sebagai panduan untuk menjalankan penelitian ini agar hasil yang dicapai tetap sesuai dengan tujuan yang telah ditetapkan sebelumnya. Berikut adalah gambaran tentang metode yang digunakan dalam penelitian ini. Gambar 1 menggambarkan langkah-langkah penerapan metode penelitian yang digunakan dalam penelitian ini.



Gambar 1. Tahapan Penelitian

2.1 Perumusan Masalah

Pada tahap ini yang akan dilakukan pada penelitian ini yaitu pengamanan file yang berada di CV Mitra Kurir Express dengan menerapkan metode enkripsi *Advanced Encryption Standard* (AES-128).

2.2 Studi Literatur

Pada tahap ini, telah dilakukan penelitian terhadap sejumlah alat dan konsep yang akan digunakan dalam penelitian ini. Penelitian juga dilakukan dengan meneliti berbagai buku pelajaran, jurnal, dan artikel ilmiah yang berhubungan dengan topik yang dibahas, yaitu kriptografi khususnya pada metode enkripsi *Advanced Encryption Standard* (AES).

2.3 Pengumpulan Data

Tahapan ini mencakup proses pengumpulan data yang diperlukan untuk merancang sistem pengamanan data. Beberapa langkah pengumpulan data yang telah dilakukan dalam proses ini adalah melalui wawancara, observasi, dan studi pustaka. Melalui tahapan-tahapan tersebut, data yang relevan dan penting telah dikumpulkan untuk membangun sistem pengamanan data yang sesuai.

2.4 Analisis Sistem

Tahap ini merupakan tahap identifikasi dan analisis masalah sistem yang disesuaikan dengan batasan yang ada. Dalam mengidentifikasi masalah tersebut, dilakukan analisis untuk memecahkan masalah penelitian ini dalam beberapa langkah. Langkah-langkah tersebut meliputi analisis data, analisis penerapan algoritma, dan analisis sistem. Proses analisis ini akan membantu untuk memahami masalah secara lebih mendalam dan menemukan solusi yang tepat untuk sistem pengamanan data yang diinginkan.

2.5 Perancangan Perangkat Lunak

Pada tahap ini, dilakukan perencanaan berdasarkan hasil analisis sistem, terutama dalam merancang modul enkripsi dan dekripsi, serta modul pendukung lainnya yang akan diintegrasikan dalam aplikasi. Selain itu, juga dilakukan perancangan antarmuka pengguna untuk memastikan aplikasi mudah digunakan dan sesuai dengan kebutuhan pengguna.

Dalam pengembangan perangkat lunak, metode konvensional yang akan digunakan adalah metode waterfall. Model ini mengikuti pendekatan linear, di mana setiap langkah harus diselesaikan sepenuhnya sebelum melanjutkan ke langkah berikutnya. Hasil dari setiap langkah dalam pengembangan perangkat lunak akan didokumentasikan dengan baik sebelum melanjutkan ke langkah selanjutnya.

2.6 Implementasi

Pada proses implementasi, dilakukan pembuatan modul-modul yang telah dirancang pada tahap perancangan ke dalam bahasa pemrograman tertentu. Dalam hal ini, aplikasi yang digunakan adalah:

1) Perangkat lunak yang digunakan dalam proses penerapan pengamanan data file menggunakan bahasa pemograman PHP serta DBMS yang digunakan adalah PHP admin.
2) Perangkat keras yang digunakan diantaranya Prosesor intel core i3, RAM 8GB, SSD 256GB.

2.7 Pengujian Sistem

Dalam tahapan pengujian sistem, dilakukan pengujian terhadap sistem yang telah dibuat dengan tujuan untuk memastikan bahwa sistem sesuai dengan hasil analisis dan apakah perancangan aplikasi telah sesuai dengan harapan. Metode pengujian yang digunakan adalah blackbox testing. Black box testing adalah metode pengujian yang digunakan untuk menemukan kesalahan dan melakukan percobaan terhadap fungsionalitas aplikasi saat dioperasikan. Tujuan utamanya adalah untuk memverifikasi apakah input yang diterima oleh aplikasi dikelola dengan benar dan output yang dihasilkan sesuai dengan yang diharapkan.

2.8 Kesimpulan

Pada tahap terakhir ini, disimpulkan bahwa penerapan metode kriptografi *Advanced Encryption Standard* (AES) 128 berfungsi dengan baik dan dapat mengamankan file pada CV Mitra Kurir Express dengan aman. Selain itu, pada tahap ini juga diajukan beberapa saran untuk perkembangan pada sistem ini.

2.9 Metode Kriptografi AES 128

Algoritma *Advanced Encryption Standard* (AES) merupakan salah satu algoritma *block chiper* yang mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Pada

tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaannya. Algoritma AES memiliki beberapa kunci yang bervariasi, yaitu 128 Bit, 192 Bit, dan 256 Bit. Perbedaan dari ketiga jenis tersebut ada pada panjang kunci yang mempengaruhi jumlah round (perputaran) yang bisa digambarkan pada gambar 2 [8].

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-129	6	4	12
AES-256	8	4	14

Gambar 2. Perbedaan 3 Jenis Algoritma AES

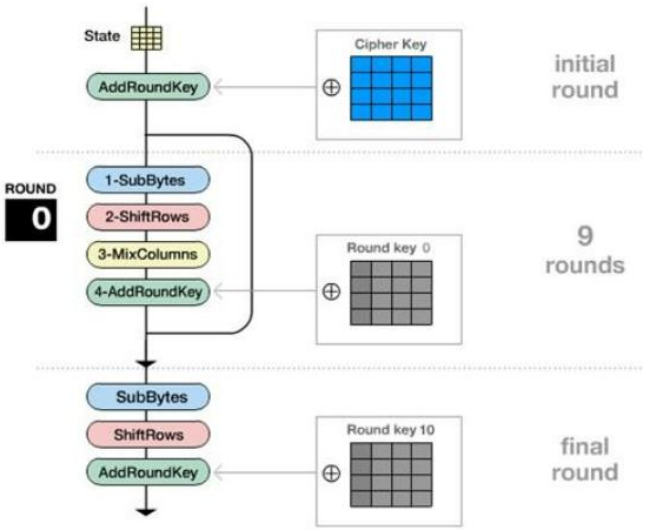
Untuk penelitian ini digunakan Metode Algoritma AES 128 Bit dengan jumlah putaran enkripsi sebanyak 10 kali. Terdapat 4 transformasi putaran pada proses enkripsi dan dekripsi: [9]

1. *SubBytes* Berfungsi untuk menukar isi dari byte dengan menggunakan tabel substitusi (S-BOX).
2. *ShiftRows* Proses pergeseran blok per baris pada *state array*.
3. *MixColumn* Proses mengalikan blok data (pengacakan) di masing-masing *state array*.
4. *array* dan *round key* dengan hubungan XOR.

Untuk proses dekripsi menggunakan tahap berikut:

1. *InvShiftRows* Melakukan pergeseran bit ke kanan pada setiap blok baris.
2. *InvSubBytes* Setiap elemen pada state dipetakan dengan tabel Inverse S-Box.
3. *InvMixColumn* Setiap kolom dalam state dikalikan dengan matriks AES.
4. *AddRoundKey* Mengkombinasikan state array dan round key dengan hubungan XOR.

Pada saat proses awal enkripsi, input file/data yang telah disalin ke dalam *state* akan melalui tahap transformasi *AddRoundKey*. Setelah proses *AddRoundKey* selesai, state akan melewati proses *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak 10 *round*/putaran. Proses tersebut dalam AES 128 Bit disebut sebagai *round function*. Pada round/putaran yang terakhir *state* tidak melewati proses transformasi *MixColumns* melainkan round/putaran akhir adalah hasil *final round* dari proses enkripsi menggunakan metode AES 128 Bit. Gambaran proses enkripsi dapat dilihat pada gambar 3 [10].



Gambar 3. Proses Enkripsi Algoritma AES 128 Bit

3. HASIL DAN PEMBAHASAN

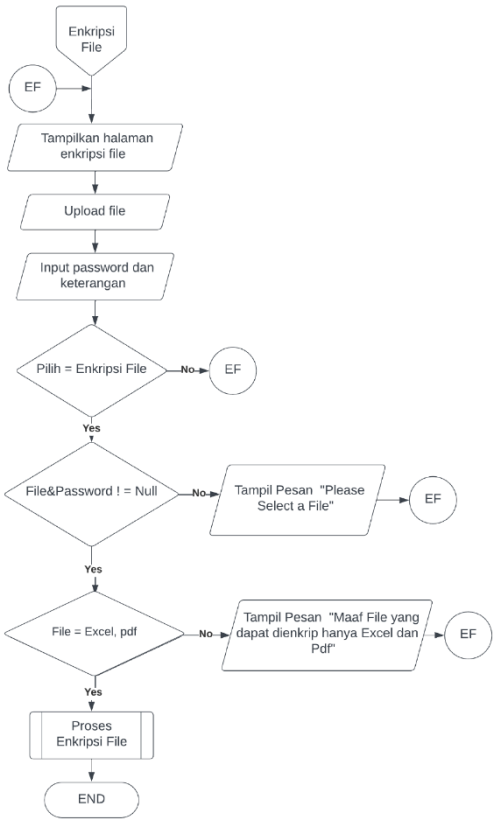
Pada bagian ini berisi analisis, hasil implementasi ataupun pengujian serta pembahasan dari topik penelitian, yang bisa dibuat terlebih dahulu metodologi penelitian. Bagian ini juga merepresentasikan penjelasan yang berupa penjelasan, gambar, tabel dan lainnya.

3.1 *Flowchart*

Flowchart adalah representasi grafis dari urutan kejadian atau langkah-langkah dalam suatu proses atau kegiatan untuk mencapai tujuan yang diharapkan. Di bawah ini terdapat flowchart yang digunakan untuk menggambarkan urutan proses dalam aplikasi pengamanan file.

3.1.1 *Flowchart* Menu Enkripsi

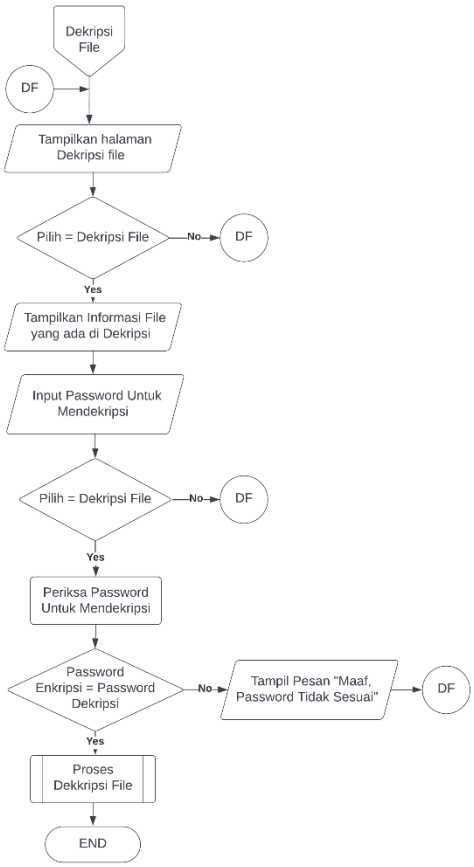
Pada Gambar 4 merupakan flowchart dari halaman enkripsi, dimana flowchart ini menjelaskan tentang cara melakukan enkripsi file. Dalam mengenkripsi file, user harus memasukkan password setelah itu program akan melakukan proses enkripsi.



Gambar 4. Flowchart Menu Enkripsi

3.1.2 *Flowchart* Menu Dekripsi

Pada gambar 5 merupakan flowchart dari halaman dekripsi, dimana flowchart ini menjelaskan tentang melakukan dekripsi file, dalam dekripsi file pengguna harus memasukkan password yang sama pada saat melakukan enkripsi file, setelah itu program akan melakukan proses dekripsi.



Gambar 5. Flowchart Menu Dekripsi

3.2 Algoritma

Pada bagian ini, akan dijelaskan algoritma yang yang ada di dalam flowchart sebelumnya. Algoritma akan disajikan dalam bentuk source code agar lebih mudah membaca dan memahaminya.

3.2.1 Algoritma Proses Enkripsi

Berikut ini merupakan algoritma untuk mengenkripsi file.

```
1.  Tampilkan Halaman Beranda
2.  Input Pilih
3.  If pilih = Enkrip File then
4.      Tampilkan Form enkripsi
5.  Input File
6.  Input Password
7.  Input Deskripsi/Keterangan
8.      If pilih = enkripsi file then
9.      If File & Password!=null then
10.     If file = xlsx, pdf then
11.     Tampilkan Pesan "file berhasil"
12. Else
13.     Tampilkan "Maaf file yang bisa dienkripsi hanya Excel dan Pdf"
14. End if
15.     Else
16.     Tampilkan Pesan "Tolong isi File"
17. End if
18. Else If pilih = Beranda then
19. Tampilkan Menu Halaman Utama
20. Return
```

3.2.2 Algoritma Proses Dekripsi

Algoritma ini menjelaskan proses form dekripsi dimana file yang telah dienkripsi akan dikembalikan ke bentuk aslinya atau didekripsi.

```
1.  Tampilkan Halaman Beranda
2.  Input Pilih
3.  If pilih = Dekripsi then
4.      Tampilkan Halaman Form Dekripsi
5.  If pilih = Dekripsi File then
6.      Tampilkan Informasi yang akan di dekripsi
7.  Input file
8.  If pilih = Dekripsi File then
9.      Periksa Password
10.         If password dekripsi = password enkripsi then
11.     Proses Enkripsi File
12.         Tampilkan File Berhasil didekripsi
13.     Else
14.         Tampilkan Password Salah
15. Else If
16. pilih = Beranda then
17. Menampilkan Halaman Beranda
18. End if
19. End if
20. End if
21. End if
22. Return
```

3.3 Tampilan Layar

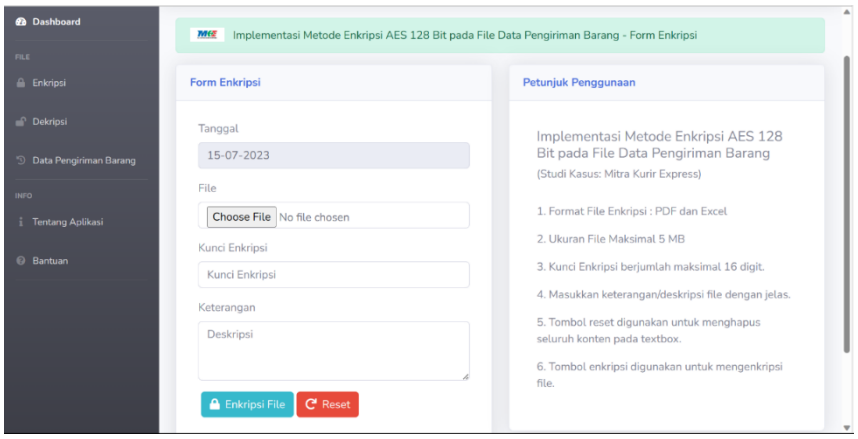
3.3.1 Tampilan Layar Menu Dashboard

Pada gambar 6 merupakan tampilan layar menu dashboard. Di dalam menu ini user dapat mengetahui berapa jumlah user, file yang telah dienkripsi, file yang terdekripsi, serta jumlah file keseluruhan.

Gambar 6. Tampilan Layar Menu Dashboard

3.3.2 Tampilan Layar Enkripsi

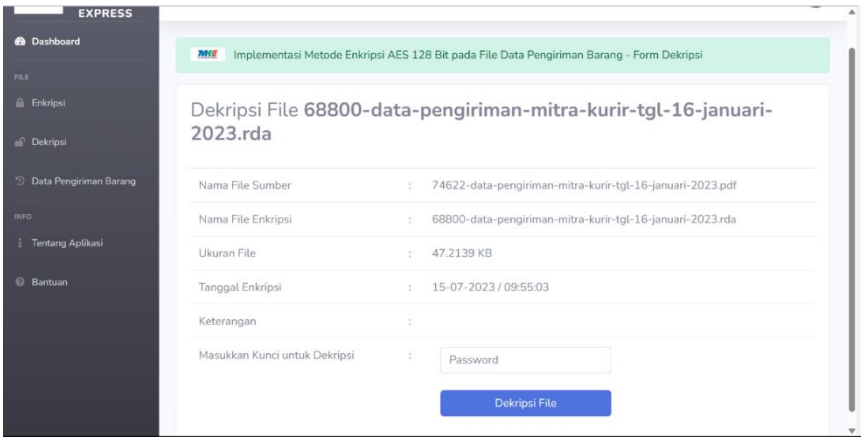
Pada gambar 7 merupakan tampilan layar halaman enkripsi. Di dalam halaman enkripsi ini, menampilan tanggal enkripsi file, choose file yang dapat digunakan untuk memilih file yang akan dienkripsi di dalam komputer, dan password untuk enkripsi file.



Gambar 7. Tampilan Layar Enkripsi

3.3.3 Tampilan Layar Dekripsi

Pada gambar 8 merupakan tampilan layar halaman proses dekripsi. merupakan rancangan layar proses dekripsi file. Pada proses dekripsi file, user harus memasukkan password yang sebelumnya digunakan untuk mengenkripsi file.



Gambar 8. Tampilan Layar Dekripsi

3.4 Pengujian

Berdasarkan hasil pengujian terhadap kecepatan dan hasil enkripsi menggunakan algoritma kriptografi AES-128 pada berbagai karakter dan ukuran data, Tabel 1 dan Tabel 2 menyajikan hasil pengujian yang telah dilakukan.

Tabel 1 Hasil Pengujian Proses Enkripsi

No	Nama File	Nama File Hasil Enkripsi	Ukuran File	Waktu
1	43953-data-pengiriman-mitra-kurir-tgl-16-januari-2023.pdf	16124-data-pengiriman-mitra-kurir-tgl-16-januari-2023.rda	48.347 byte	25.020 milidetik
2	56443-data-pengiriman-mitra-kurir-tgl-16-januari-2023.xls	6982-data-pengiriman-mitra-kurir-tgl-16-januari-2023.rda	72.704 byte	56.890 milidetik
			Rata-rata waktu enkripsi file	40.955 milidetik

Tabel 2 Hasil Pengujian Proses Dekripsi

No	Nama File	Nama File Hasil Enkripsi	Ukuran File	Waktu
1	16124-data-pengiriman-mitra-kurir-tgl-16-januari-2023.rda	43953-data-pengiriman-mitra-kurir-tgl-16-januari-2023.pdf	48.347 byte	160 milidetik
2	6982-data-pengiriman-mitra-kurir-tgl-16-januari-2023.rda	56443-data-pengiriman-mitra-kurir-tgl-16-januari-2023.xls	72.704 byte	12430 milidetik
			Rata-rata waktu dekripsi file	6.295 milidetik

4. KESIMPULAN

Setelah melakukan perancangan dan pengembangan aplikasi kriptografi berbasis web untuk proses enkripsi dan dekripsi file, serta menangani permasalahan yang telah dibahas sebelumnya, maka dapat disimpulkan bahwa aplikasi kriptografi berbasis web berhasil dibangun dan dapat digunakan untuk melakukan proses enkripsi dan dekripsi file dengan menggunakan metode Advanced Encryption Standard (AES-128). Hasil akhir pengujian rata-rata waktu yang dibutuhkan untuk proses enkripsi file yaitu 40.955 milidetik dan rata-rata waktu yang dibutuhkan untuk proses dekripsi file yaitu 6.295 milidetik. Untuk pengembangan selanjutnya diharapkan aplikasi ini dapat beroperasi pada sistem operasi android, ios, dll.

DAFTAR PUSTAKA

[1] Auliyah, A. I. "Implementasi Kombinasi Algoritma Enkripsi Rivest Shamir Adleman (Rsa) dan Algoritma Kompresi Huffman Pada File Document". Indonesian Journal of Data and Science, 1(1), 23-28, 2020

[2] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)". Jurnal Pendidikan Sains dan Komputer, 2(01), 163-171, 2022.

[3] Nuari, R., Ratama, N., Informatika, J. T., Teknik, F., & Pamulang, U. "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping". Journal Of Artificial Intelligence And Innovative Applications, 1(2), 37-44, 2020.

[4] Sitorus, F. A., Nugroho, N. B., & Pane, U. F. S. S. "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. MITSUBISHI ELECTRIC INDONESIA". Jurnal Cyber Tech, 4(5), 2022.

[5] Putri, A. E., Kartikadewi, A., & Rosyid, L. A. "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang". Appl. Inf. Syst. Manag, 3(2), 69-78, 2021

[6] Mustika, L. "Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web". JURIKOM (Jurnal Riset Komputer), 7(1), 148-155, 2020.

[7] Hanadwiputra, S. Implementasi Enkripsi Dalam Pengamanan File Data Karyawan Dengan Metode Algoritma DES (Data Encryption Standard) Pada CV. Sinergi Informasi Global. Gema Kampus IISIP YAPIS Biak, 13(2), 61-69, 2018.

[8] Prameshwari, A., & Sastra, N. P. "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen". Jurnal Eksplora Informatika, 8(1), 52-58, 2018.

[9] Cristy, N., & Riandari, F. "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan". Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), 4(2), 75-85, 2021.

[10] Novianti, H. D., & Hidayat, A. T. "Implementasi Kriptografi Advanced Encryption Standard 128 Bit dalam Pengamanan Data Keuangan Kas". Jurnal Komputer dan Teknologi, 27-34, 2023.