4thSeminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
27 Maret 2024 – Jakarta, Indonesia
Volume 3, Nomor 1, April 2024 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITME AES-128 UNTUK ENKRIPSI DAN DEKRIPSI FILE DOKUMEN BERBASIS WEB PADA LAW OFFICE ERDI SURBAKTI, S.H & REKAN

Pedrolin Suranta Surbakti[1], Purwanto[2]

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

Email: [1]1911502415@ budiluhur.ac.id, [2]purwanto@budiluhur.ac.id
(* : corresponding author)

Abstrak- Pesatnya perkembangan teknologi informasi telah memudahkan masyarakat dalam bertukar informasi baik berupa file maupun data rahasia. Tingginya kasus kebocoran data pribadi di dunia digital yang disalah gunakan oleh oknum yang tidak bertanggung jawab untuk dijual. Rendahnya kualitas keamanan dari suatu file menjadi permasalahan yang sering terjadi. Dalam implementasi ini, dokumen yang dapat digunakan adalah dokumen dengan format docx, xlsx, pptx, dan pdf. Sistem yang dikembangkan memastikan bahwa data dalam dokumen tersebut tidak dapat dibaca atau dimodifikasi oleh pihak yang tidak berwenang. Pengamanan informasi pada dasarnya berfungsi untuk memastikan bahwa orang yang tidak berhak tidak dapat membaca, mengubah, atau menghapus informasi tersebut. Keamanan file menggunakan metode algoritma Advanced Encryption Standard 128, namun file masih tersimpan di folder atau flash disk di komputer, sehingga saat ini belum aman. Tujuan dari penelitian ini adalah untuk mengaktifkan keamanan file dengan mengubah isi suatu file dari dapat dibaca menjadi tidak dapat dibaca, atau dari tidak dapat dibaca menjadi dapat dibaca seperti sebelumnya. Aplikasi keamanan file yang menggunakan algoritma enkripsi berbasis web. Algoritma Advanced Encryption Standard (AES-128) adalah algoritma untuk melindungi file. Akibatnya, file sebelum dan sesudah enkripsi dan dekripsi tidak rusak dalam proses apapun.

Kata Kunci: Kriptografi, data, Advanced Encryption Standard (AES-128).

Abstract- *The rapid development of information technology has made it easier for people to exchange information in the form of files and confidential data. There are high cases of leaks of personal data in the digital world which are misused by irresponsible individuals for sale. Low security quality of a file is a problem that often occurs. In this implementation, documents that can be used are documents in docx, xlsx, pptx and pdf formats. The system developed ensures that the data in the document cannot be read or modified by unauthorized parties. Information security basically functions to ensure that unauthorized people cannot read, change or delete the information. File security uses the Advanced Encryption Standard 128 algorithm method, but files are still stored in folders or flash disks on the computer, so they are not safe at this time. The aim of this research is to enable file security by changing the contents of a file from readable to unreadable, or from unreadable to readable as before. File security application that uses web-based encryption algorithms. The Advanced Encryption Standard (AES-128) algorithm is an algorithm for protecting files. As a result, files before and after encryption and decryption are not damaged in any process.*

Keywords*: Cryptography, file, Advanced Encryption Standard (AES-128).*

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi saat ini berkembang sangat pesat. Pengolahan dan pendistribusian informasi melalui jaringan telekomunikasi membuka berbagai kemungkinan penerapannya di berbagai bidang kehidupan manusia. Salah satu contohnya adalah penggunaan jaringan internet, yang memungkinkan orang untuk bertukar dokumen atau data satu sama lain[1]. Seiring dengan berkembangnya teknologi tersebut, banyaknya kasus pencurian data pribadi oleh oknum yang tidak bertanggung jawab di dunia digital didorong oleh nilai jual data pribadi yang tinggi serta menyalahgunakan teknologi informasi untuk mengakses data atau dokumen tanpa izin dari pihak terkait. Orang-orang yang melakukan tindakan tersebut dikenal sebagai hacker, cracker, carder, dll. Problemnya adalah bahwa kasus cybercrime data keamanan informasi menjadi sangat penting di era teknologi saat ini. Misalnya, pada tahun 2014, jumlah kejahatan sebanyak 1225, dengan persetujuan kejahatan 790, yang mewakili 64% dari kasus, pada tahun 2015, jumlah kejahatan sebesar 1569, dengan persetujuan kejahatan 851, dan pada tahun 2016, jumlah kejahatan sebesar 1207, dengan persetujuan kejahatan 699, yang mewakili 57% dari kasus.. Oleh karena itu, diperlukan pengamanan data atau dokumen tersebut dengan cara menjaga kerahasiaan informasi yang terdapat dalam kriptografi[2].

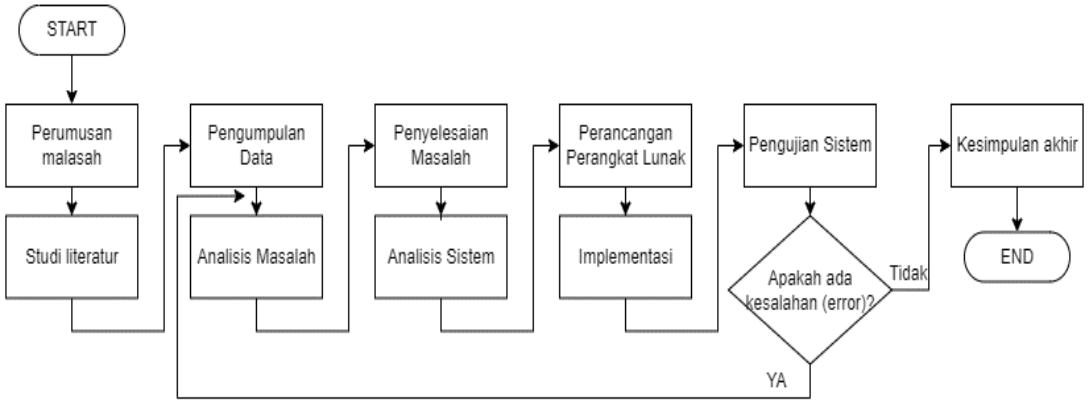
Kriptografi adalah ilmu komputer yang bertujuan untuk melindungi data. Enkripsi dapat diartikan sebagai ilmu atau seni menjaga keamanan pesan. Menggunakan dua langkah enkripsi dasar: enkripsi dan dekripsi[3].

Proses enkripsi melibatkan penggunaan kunci untuk mengubah atau mengenkripsi pesan asli yang dikirim menjadi informasi acak. Plaintext penerima dapat diperoleh dengan menggunakan kunci ini untuk mendekripsi ciphertext. [4]. Proses menyembunyikan data atau mengubah teks biasa menjadi teks sandi disebut enkripsi, sementara untuk mengembalikan teks sandi menjadi teks biasa disebut dekripsi. enkripsi memungkinkan mengubah pesan yang dapat dimengerti menjadi pesan yang tidak dapat dimengerti dengan menggunakan algoritme[5].

Adapun tujuan dari penelitian ini yaitu mengetahui konsep kriptografi untuk pengamanan data berbasis *file* dengan menggunakan algoritme AES-128. Algoritme AES akan digunakan untuk proses enkripsi dan dekripsi dalam pengembangan sistem. Pada tahun 2001, National Institute of Standards and Technology (NIST) sebagai agensi departemen perdagangan Amerika Serikat menetapkan sebuah standard kriptografi yang baru yaitu Algoritma Rijandel dan ditetapkan sebagai Advanced Encryption Standard (AES) Algoritme AES ini memiliki tiga faktor penilaian yang lebih unggul daripada versi sebelumnya, yaitu Data Encryption Standard (DES) [6]. Tahap pembuatan aplikasi keamanan file berbasis web berbasis PHP dengan database MySQL. Hasil implementasi menunjukkan bahwa aplikasi dapat mengubah file yang semula berbentuk plaintext menjadi chipertext, dengan hasil akhir file yang tidak lagi dapat dipahami. Hasil akhir menunjukkan bahwa penerapan metode enkripsi Advanced Encryption Standard (AES) 128 berhasil, dan aplikasi dapat menjaga, melindungi, dan mencegah serangan hacker dan kebocoran data pada LAW OFFICE ERDI SURBAKTI & REKAN

2. METODE PENELITIAN

Pendekatan penelitian ini menggunakan metode *waterfall*, yaitu pertanyaan penelitian ditetapkan dan dilakukan tinjauan literatur dengan membaca publikasi penelitian sebelumnya untuk memastikan temuan tetap sesuai dengan tujuan penelitian. Gambar 1 menunjukkan langkah-langkah yang diperlukan untuk menerapkan metodologi penelitian yang digunakan dalam penelitian ini.



Gambar 1. Tahapan Penelitian

a. Studi Literatur

Melakukan studi pustaka dengan membaca buku digital, jurnal, dan referensi lain yang terkait dengan teori kriptografi, teori pengamanan file, teori dari metode AES, dan teori-teori pendukung lainnya.

1) Wawancara (Interview)

Lakukan wawancara dengan pihak terkait untuk memperoleh informasi tentang kebutuhan system pengamanan file untuk data penggajian dan data diri karyawan.

2) Observasi (Observation)

Kumpulkan data dan lakukan pengamatan langsung di LAW OFFICE ERDI SURBAKTI SH&REKAN untuk menjadi masukan dalam laporan penelitian.

2.1 Rancangan Pengujian

Algoritma kriptografi Advanced Encryption Standard 128 (AES128) akan digunakan untuk menjalankan pengujian. Aplikasi ini akan membuat menu login di mana orang harus memasukkan username dan password mereka saat ingin menggunakannya. Setelah masuk ke akun, pengguna akan langsung dibawa ke menu dashboard, yang berisi informasi tentang informasi LAW OFFICE ERDI SURBAKTI SH&REKAN. Di bagian bawah halaman, ada tombol menu yang menampilkan submenu, yang memiliki tombol untuk enkripsi, deskripsi, dan daftar berkas. Tombol enkripsi dapat digunakan untuk memulai enkripsi file tertentu, dan tombol dekripsi dapat digunakan untuk mendekripsi file yang telah dienkripsi sebelumnya. Daftar hasil untuk melihat hasil file yang sudah dienkripsi atau didekripsi dan didalam daftar berkas juga bisa mengunduh hasil enkripsi dan dekripsi. Menu logout jika di klik, maka akan langsung diarahkan kembali ke halaman login. Pada penelitian ini penulis

menggunakan blackbox Testing untuk proses pengujian pada program (Tabel 1), dimana dilakukan dengan mengamati hasil eksekusi menggunakan data uji perangkat lunak dan uji fungsional.

Table 1. Rancangan Pengujian

No	Test Case	Hasil Pengujian
1.	Tombol Login	Tampil halaman menu dashboard
2.	Tombol Enkripsi	Menampilkan tampilan halaman Enkripsi
3.	Tombol Choose File	Memilih file yang ingin dienkripsi
4.	Tombol Ekripsi Berkas	Memilih berkas yang ingin di enkripsi
5.	Tombol Dekripsi	Menampilkan tampilan halaman Enkripsi
6.	Tombol Dekripsi Berkas	Dapat Mengdekripsikan berkas yang sudah diupload
7.	Tombol Daftar Hasil	Menampilkan File yang sudah dienkripsi / dekripsi
8.	Tombol Logout	Kembali ke halaman login

2.2 Rancangan Basis Data

Desain basis data mencakup diagram kelas, logical record structure (LRS), dan spesifikasi basis data. Penelitian ini menggunakan diagram kelas. Diagram kelas menjelaskan struktur dan hubungan antar objek dalam aplikasi Anda. Struktur ini berisi atribut dan metode kelas.

2.3 Kriptografi

Kriptografi klasik, yang menggunakan kertas, pensil, atau perangkat mekanis sederhana, adalah dasar kriptografi. Secara umum, algoritma kriptografi klasik terbagi menjadi dua kategori: algoritma enkripsi transposisi dan algoritma enkripsi permutasi. Sandi substitusi menggantikan setiap karakter atau kelompok karakter dengan karakter atau kelompok karakter lain, tetapi sandi transposisi mengubah urutan karakter dalam pesan[7].

2.4 AES (*Advanced Encryption Standard*)

Algoritma AES merupakan metode enkripsi yang diterbitkan oleh NIST (National Institute of Standards and Technology) pada tahun 2001 untuk menggantikan algoritma DES yang dianggap sudah tua dan sangat mudah untuk diretas. Oleh karena itu, algoritma AES telah menggantikan algoritma DES sebagai standar perlindungan data. Algoritma AES merupakan jenis block cipher dengan panjang kunci 128 bit, 192 bit, dan 256 bit. Urutan kelompok algoritma AES sebanyak 128 bit merupakan suatu blok data atau sering disebut dengan plaintext yang kemudian dienkripsi menjadi ciphertext. Panjang kunci yang berbeda mempengaruhi jumlah putaran pada algoritma AES.

2.5 Metode Kriptografi AES 128

Algoritma blok cipher yang memiliki sifat simetris yang menggunakan kunci simetris selama proses enkripsi dan dekripsi. Proses berulang yang disebut Round digunakan untuk enkripsi AES. Panjang kunci yang digunakan menentukan jumlah putaran AES yang digunakan. Untuk setiap putaran, Anda harus menggunakan tombol putaran dan memasukkan input dari putaran berikutnya. Menurut kunci yang ditentukan, kunci bulat dibuat. Algorithma AES dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang berbeda, seperti 128 bit, 192 bit, dan 256 bit. Jumlah putaran yang dihasilkan dipengaruhi oleh panjang kunci. Gambar 2 menunjukkan perbedaan antara ketiga kunci tersebut, yang membandingkan jumlah kunci AES[4].

Tipe	Jumlah Key (Nk)	Besar Blok (Nb)	Jumlah Round (Nr)
AES-128	4	4	10
AES-192	5	4	12
AES-256	6	4	14

Gambar 2. Jumlah Putaran AES

Dengan panjang kunci 128 bit maka terdapat sebanyak 2128= 3,4 x 1038 kemungkinan kunci. Seperti pada DES, Rijndael atau AES menggunakan substitusi dan permutasi dan sejumlah putaran atau cipher berulang. Dalam setiap putaran menggunakan kunci internal yang berbeda. Proses enkripsi AES-128 dengan kunci 128 bit adalah sebagai berikut:

1. AddRoundKey: melakukan XOR antara keadaan awal (teks biasa) dan kunci enkripsi. Fase ini disebut juga babak pertama.

2. Round : Putaran nomor satu kali. Proses berikut dilakukan pada setiap putaran: 1) SubBytes: Substitusi byte menggunakan tabel substitusi, juga dikenal sebagai S-box.
3. ShiftRows memungkinkan pergeseran baris-baris array state melalui bungkus..
4. MixColumns : mengacak data di setiap kolom array keadaan menggunakan persamaan berikut: A(x) = {03}x2 + {01}x2 + {01}x2 + {02 } (1)
5. Babak Final : Proses babak final meliputi : 1) SubBytes 2) ShiftRows 3) AddRoundKey
6. Pada proses akhir menghasilkan karakter atau teks berupa ciphertext [8].

Proses dekripsi AES-128 dengan kunci 128 bit adalah sebagai berikut:

1. InvShiftRows : melakukan sedikit pergeseran ke kanan pada setiap blok baris.
2. InSubBytes : Setiap elemen status ditugaskan ke tabel S-box terbalik.
3. InvMixColumns : Setiap kolom status dikalikan dengan matriks AES.
4. AddRoundKey : Menggabungkan array status dan kunci bulat dengan hubungan XOR.
5. Pada proses terakhir menghasilkan teks atau karakter asli[9].

Kelebihan AES: Menurut artikel, AES memiliki beberapa kelebihan, seperti [10]:

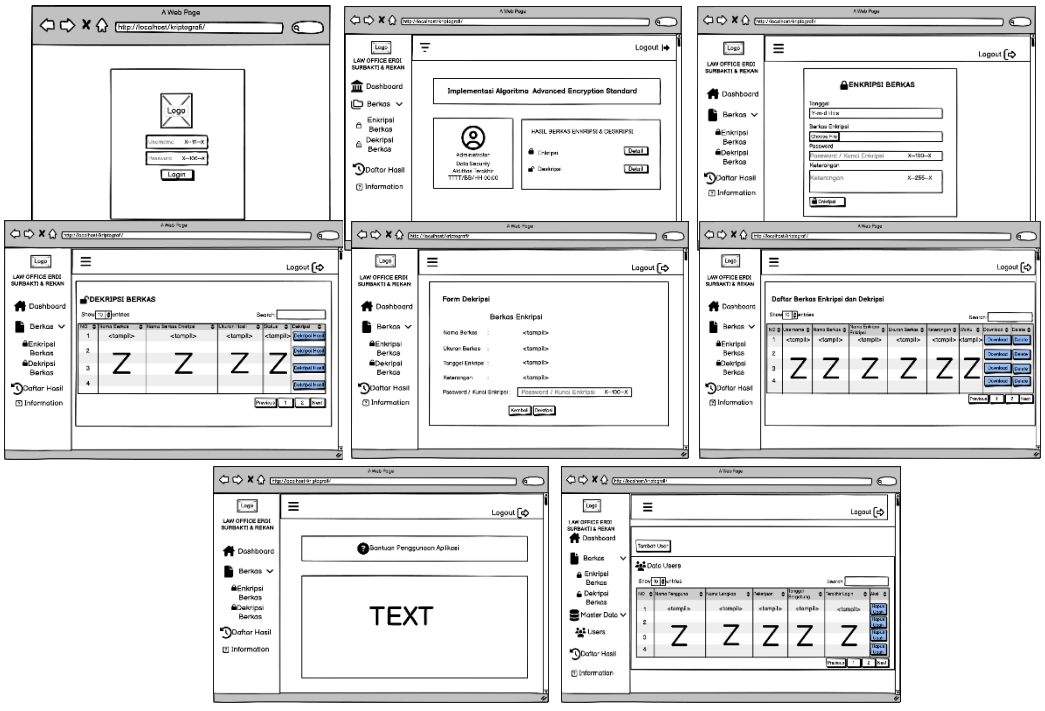
1. larangan kunci minimal pada AES adalah 128 bit. Sehingga dengan teknologi yang sekarang, AES tahan terhadap serangan exhaustive key lookup. Dengan panjang kunci 128bit adalah 2128 ≈ 3,4 x 1038 kemungkinan larangan.
2. Sifat karakteristik bidang GF (28), di mana selalu ada satu bidang khusus untuk setiap bilangan prima, menyebabkan kekuatan AES. Dengan demikian, semua representasi GF (28) adalah isomorfik dan pemilihan polynomial biner derajat 8.

Kelemahan AES: Menurut artikel, AES memiliki beberapa kelemahan, termasuk:

1. Manajemen kunci menjadi sulit dengan jenis kunci simetris karena pengguna memerlukan kunci yang berbeda untuk setiap pengiriman dan penerimaan data.
2. AES adalah salah satu algoritma kriptografi yang menggunakan tipe kunci simetris dalam proses pengiriman dan penerimaan data. Ini membuat kunci simetris mudah bocor dalam waktu yang lama.

2.6 Rancangan Layar

Desain ini selalu diperlukan saat merancang sebuah aplikasi. Desain layar adalah langkah pertama dalam menciptakan tampilan dan nuansa aplikasi Anda yang diinginkan. Tujuan dari desain layar adalah untuk membuat tampilan lebih mudah dibuat.



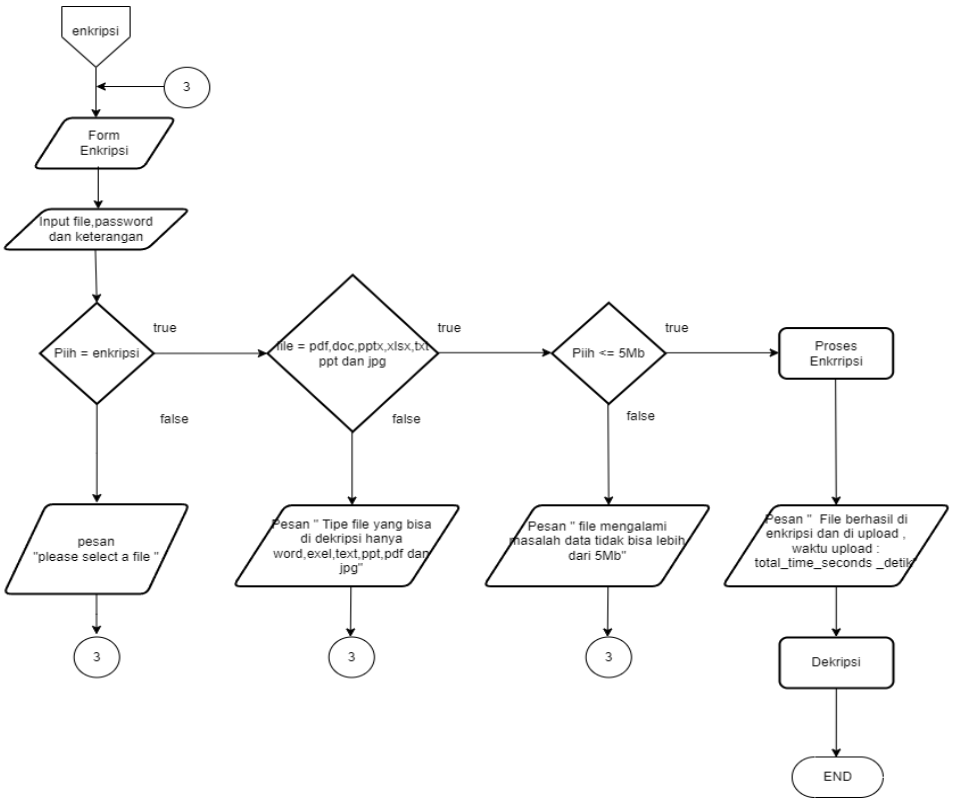
3. HASIL DAN PEMBAHASAN

Berdasarkan metode yang akan datang, algoritme kriptografi AES-128 digunakan untuk mengenkripsi dan dekripsi dokumen. Diagram aliran, algoritme, prosedur, dan hasil dari enkripsi dan dekripsi dokumen pada aplikasi akan dijelaskan dalam implementasi ini.

.

3.1 Flowchart From Enkripsi

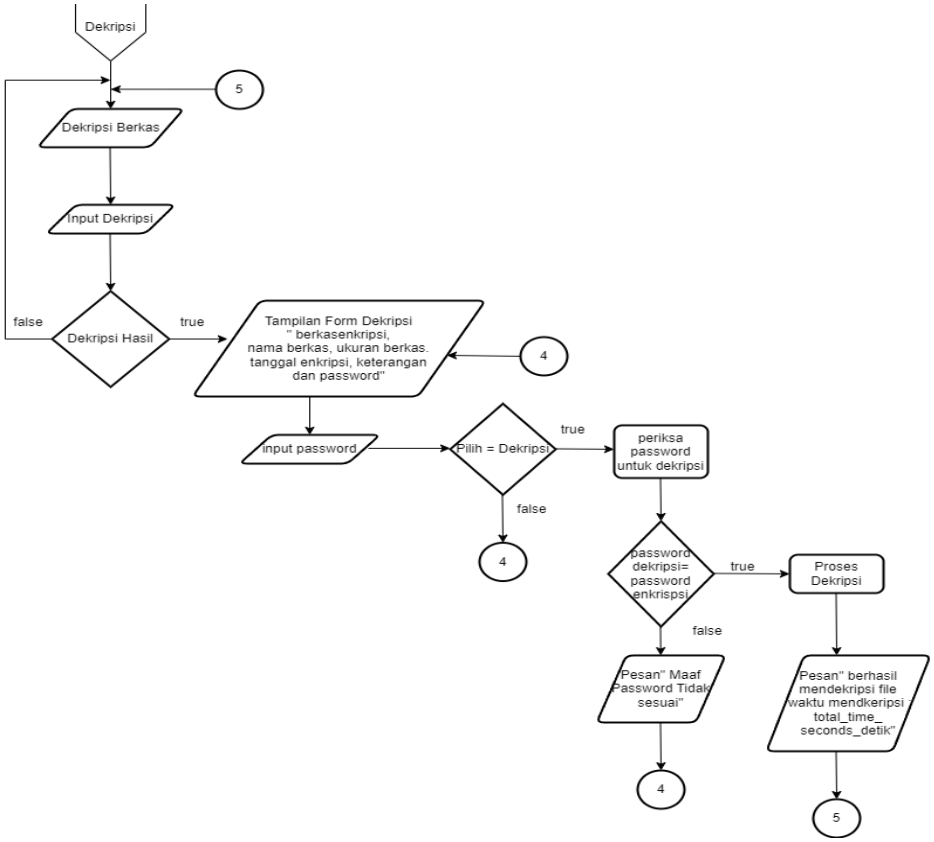
Flowchart From Enkripsi adalah alur proses suatu form yang terdapat pada program, form ini memperlihatkan alur proses untuk melakukan enkripsi file. Proses enkripsi ini di wajibkan untuk memasukan password. Berikut di bawah ini Flowchart Form Enkripsi.



Gambar 4. Flowchart Proses Enkripsi

3.2 Flowchart Form Dekripsi

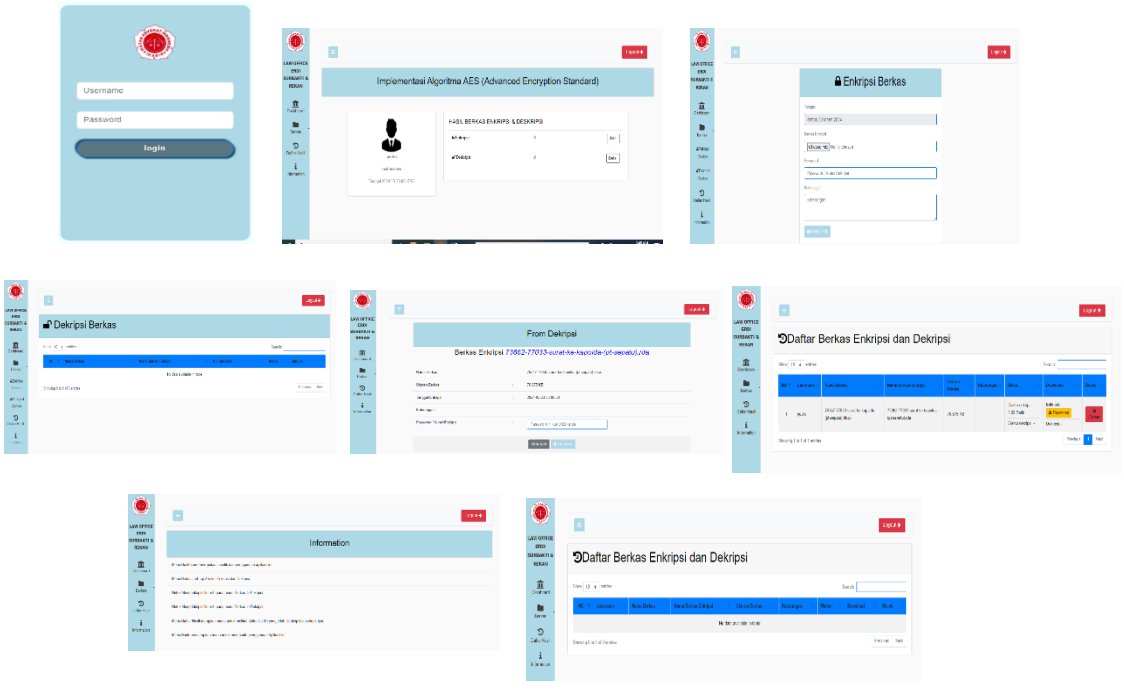
Flowchart Form dekripsi adalah suatu urutan proses untuk melakukan dekripsi file yang sudah di enkripsi sebelumnya. Untuk melakukan suatu proses dekripsi pengguna di wajibkan memasukan passoword yang sama pada saat pengguna melakukan enkripsi. Berikut di bawah ini Flowchart Form Dekripsi.



Gambar 5. Flowchart Proses Dekripsi

3.3 Tampilan Layar

Layar ini menampilkan layar yang disertakan dalam program. Berikut tampilan layar dan penjelasannya.



3.4 Pengujian

Berikut hasil pengujian file asli dengan file terenkripsi menggunakan aplikasi ini dan memenuhi persyaratan spesifikasi perangkat lunak dan perangkat keras.

Table 2. Hasil Pengujian Enkripsi

NO	Nama File Awal	Ukuran File	Nama File Hasil Enkripsi	Ukuran File Setalah Enkripsi	Status	
					Durasi Enkripsi	Keterangan
1	SURAT KE KAPOLDA (PT SEPATU).docx	77 KB	22397-surat-ke-kapolda-(pt-sepatu).rda	76.8 KB	6.42 detik	BERHASIL
2	1_proses enkrip dan dekrip.txt	2 KB	7627-1_proses-enkrip-dan-dekrip.rda	1.25 KB	0.06 detik	BERHASIL
3	SURAT KE INSPEKTORAT BPN.pdf	35 KB	69041-surat-ke-inspektorat-bpn.rda	34.3 KB	1.08 detik	BERHASIL
4	PERMOHONAN EKSEKUSI (232,RYANTO,JAKTIM).docx	67 KB	46999-permohonan-eksekusi-(232,ryanto,jaktim).rda	66.7 KB	2.12 detik	BERHASIL
5	Exel Asesment ZEA.xlsx	15 KB	46485-excel-asesment-zea-(1).rda	14.18 KB	0.59 detik	BERHASIL
6	PPT_SKRIPSI_PEDRO.pptx	3.276 KB	61068-ppt_skripsi_pedro.rda	3.275 KB	101.91 detik	BERHASIL

Dalam pengujian enkripsi hasil dari serangkaian pengujian terkait proses enkripsi berkas bahwa pengujian ukuran berkas tidak mengalami perubahan yang signifikan dan dalam proses enkripsi tidak memakan waktu saat dilakukan proses enkripsi hal ini menggambarkan keefisienan dan konsistensi sistem kami dalam menjalankan proses enkripsi pada variasi berkas yang berbeda.

Table 3. Hasil Pengujian Dekripsi

NO	Nama File Enkripsi	Ukuran File Enkripsi	Nama File Hasil Dekripsi	Ukuran File Dekripsi	Status	
					Durasi Enkripsi	Keterangan
1	22397-surat-ke-kapolda-(pt-sepatu).rda	76.86 KB	77033-surat-ke-kapolda-(pt-sepatu).docx	77 KB	6.87 detik	BERHASIL
2	7627-1_proses-enkrip-dan-dekrip.rda	1.25 KB	73638-1_proses enkrip-dan-dekrip.txt	2 KB	0.06 detik	BERHASIL
3	69041-surat-ke-inspektorat-bpn.rda	34.30 KB	62175-surat-ke-inspektorat-bpn.pdf	35 KB	1.19 detik	BERHASIL
4	46999-permohonan-eksekusi-(232,ryanto,jaktim).rda	66.76 KB	39845-permohonan-eksekusi-(232,ryanto,jaktim).docx	67 KB	2.14 detik	BERHASIL
5	46485-excel-asesment-zea-(1).rda	14.18 KB	73243-excel-asesment-zea-(1).xlsx	15 KB	0.59 detik	BERHASIL

6	61068-ppt_skripsi_pedro.rda	3.275 KB	94697-ppt_skripsi_pedro.pptx	3.276 KB	107.1 detik	BERHASIL

Berdasarkan bagian proses pengujian dekripsi berkas, tidak terlihat adanya perubahan dalam ukuran berkas setelah proses dekripsi selesai. Lebih menarik lagi, waktu yang dibutuhkan untuk melaksanakan dekripsi ternyata sama dengan waktu yang diperlukan dalam proses sebelumnya. Hal ini mengindikasikan efisiensi dan konsistensi dari sistem kami dalam menjalankan proses dekripsi pada berbagai jenis berkas.

4. KESIMPULAN

Berdasarkan analisis dan uraian yang telah dilakukan, maka dapat disimpulkan pada Law Office Erdi Subakti SH&Rekan dapat diimplementasikan aplikasi berbasis web dengan kriptografi pengamanan file menggunakan algoritma Advanced Encryption Standard (AES-128). Pada aplikasi ini penulis berhasil mengamankan dokumen pada Law Office Erdi Subakti SH&Rekan dengan sistem kriptografi yang berbasis website pengamanan file ini dapat berhasil melakukan proses enkripsi dan dekripsi dan tidak mengubah ukuran pada file data asli. Sistem kriptografi yang berbasis website ini diharapkan dapat melakukan pengamanan selain file yang ekstensi .xlsx, .pptx, .docx, .txt dan pdf. sehingga file yang berformat lain dapat dilakukan pengamanan dan terhindar dari penyalahgunaan data. Penelitian selanjutnya diharapkan dapat mengkombinasikan metode kriptografi lain dalam pengamanan file agar keamanan data yang dilakukan lebih aman dan tidak mudah untuk dibuka oleh pihak lain yang tidak bertanggung jawab.

b. DAFTAR PUSTAKA

[1] I. Kriptografi, A. Rc, and D. A. N. Dan, “Steganografi Dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop Pada Smk As- Su ’ Udiyyah,” vol. 3, no. 4, pp. 54–60, 2020.

[2] 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.

[3] F. D. Yonathan, H. Nasution, and H. Priyanto, “Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid dan Algoritma Kompresi Huffman,” *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 2, p. 181, 2021, doi: 10.26418/jp.v7i2.47077.

[4] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, “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.*, vol. 3, no. 2, pp. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[5] N. Berliano, N. Putra, F. A. Raihana, and W. M. Albert, “Analisis Enkripsi Kriptografi Asimetris Algoritma RSA Berbasis Pemrograman Batch pada Media Flashdisk,” vol. 8, pp. 142–154, 2023.

[6] H. Wijaya, “Jurnal Akademika Penerbit Implementasi Kriptografi Aes-128 Untuk Mengamankan Url (Uniform Resource Locator) Dari Sql Injection,” *J. Akad.*, vol. 17, no. 1, pp. 8–13, 2020, [Online]. Available: https://www.ejournal.lppmunidayan.ac.id/index.php/akd

[7] 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.

[8] N. Sijabat, N. Hayaty, and E. Suswaini, “Implementasi Kriptografi Hybrid Menggunakan Algoritma AES-128 dan Algoritma Rabin untuk Mengamankan Data dalam Database,” *Student Online Joernal*, vol. 3, no. 1, pp. 178–183, 2022.

[9] N. U. Baidoi, M. Hardjianto, and A. Wibowo, “IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD UNTUK PENGAMANAN FILE PADA SMP NEGERI 189 JAKARTA BARAT IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD ALGORITHM FOR SECURING FILES AT SMP NEGERI 189 WEST,” vol. 2, no. April, pp. 1–9, 2023.

[10] N. W. Hidayatulloh, M. Tahir, H. Amalia, N. A. Basyar, A. F. Prianggara, and M. Yasin, “Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data,” vol. 3, no. 1, pp. 1–10, 2023.