Jurnal TICOM: Technology of Information and Communication
Volume 12, Nomor 3, Mei 2024 Hal: 91-96 E-ISSN: 2962-7982

Implementasi Algoritme Kriptografi *Advanced Encryption Standard* (AES-128) untuk Pengamanan Data Berbasis Web pada McDonald's Cabang T.B. Simatupang

Arif Alvian Winata[1], Mohammad Syafrullah[2], Irawan[3*]

[1,2,3]Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia
Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan, Jakarta Selatan, 12260
E-mail: [1]arif.alvian48@gmail.com, [2]mohammad.syafrullah@budiluhur.ac.id, [3*]irawan@budiluhur.ac.id
(*: corresponding author)

Abstrak - **Keamanan data atau informasi sangat penting saat menggunakan jaringan internet. Penyadapan data atau informasi dalam konteks ini bisa sangat merugikan. Keamanan informasi menjadi prioritas utama dalam era digital, di mana pertukaran informasi terjadi secara masif dan cepat. Penelitian ini menggunakan data pelanggan dan beberapa dokumen lainnya dari McDonald's TB Simatupang. Saat ini, menjaga keamanan pertukaran informasi menjadi sangat penting. Penelitian ini mengimplementasikan algoritme enkripsi AES-128 menggunakan metode waterfall untuk mengenkripsi dan mendekripsi data dalam format dokumen *Microsoft office* dan pdf. Algoritme Advanced Encryption Standard (AES) digunakan sebab menawarkan tingkat keamanan yang tinggi. Penelitian ini bertujuan untuk mengintegrasikan AES-128 di McDonald's TB Simatupang sebagai solusi keamanan data sensitif dan mencapai standar keamanan yang optimal. Penerapapan penggunaan algoritma ini adalah pilihan yang tepat untuk mengamankan data sensitif di McDonald's TB Simatupang. Hasil penelitian diuji dengan teknik pengujian black box dan dilaksanakan sesuai rencana.**

Kata Kunci - **Makanan Cepat saji, Kriptografi, Advanced Encryption Standard (AES-128), Plaintext, Chipertext.**

Abstract - **Data or information security is crucial when using the internet. Eavesdropping on data or information in this context can be highly detrimental. Information security has become a top priority in the digital era, where the exchange of information happens massively and rapidly. This research utilizes customer data and several other documents from McDonald's TB Simatupang. Currently, safeguarding the exchange of information is of utmost importance. This study implements the AES-128 encryption algorithm using the waterfall method to encrypt and decrypt data in Microsoft Office and PDF document formats. The Advanced Encryption Standard (AES) algorithm is employed because it offers a high level of security. The research aims to integrate AES-128 at McDonald's TB Simatupang as a solution for securing sensitive data and achieving optimal security standards. Implementing this algorithm is the right choice for protecting sensitive data at McDonald's TB Simatupang. The results of the study were tested using black box testing techniques and were conducted as planned.**

Keywords - ***Fast Food, Kriptografi, Advanced Encryption Standard (AES-128), Plaintext, Chipertext.***

I. PENDAHULUAN

Melindungi data dan informasi saat beraktivitas di internet adalah hal yang sangat penting. Melindungi data dan informasi sensitif di era digital memerlukan penerapan teknik enkripsi dan dekripsi. Teknik enkripsi dan dekripsi berfungsi untuk mengamankan pesan dan data agar tidak terbaca oleh pihak yang tidak berwenang. Kriptografi merupakan ilmu yang mempelajari teknik-teknik enkripsi dan dekripsi untuk mengamankan data dan informasi. [1]

Kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata: kripto yang berarti menyembunyikan dan graphia yang berarti tulisan. Ilmu ini mempelajari teknik-teknik matematika yang berkaitan dengan keamanan informasi, meliputi kerahasiaan, keabsahan, integritas, dan autentikasi data. Meskipun demikian, kriptografi tidak dapat menyelesaikan semua aspek keamanan informasi.[2] Istilah "kriptografi" berakar dari bahasa Yunani, tersusun dari kata "crypto" yang berarti "rahasia" dan "graphia" yang berarti "tulisan". Oleh karena itu, kriptografi dapat dimaknai sebagai "seni menulis rahasia". [3] Kriptografi hadir untuk menawarkan layanan keamanan penting, di antaranya melindungi komunikasi dari penyadapan oleh pihak yang tidak berwenang, menjamin keaslian dan integritas data, serta memverifikasi identitas pengguna. [4]

Advanced Encryption Standard (AES) adalah algoritma enkripsi kunci yang umumnya populer digunakanhingga kini. Algoritma ini bekerja dengan membagi data teks menjadi blok-blok berukuran 128 bit. Prosesnya dilanjutkan dengan mengubah setiap blok data menjadi matriks berukuran 4x4 yang berisi nilai-nilai heksadesimal, dan matriks ini disebut "state". Elemen-elemen state ini kemudian diubah melalui transformasi matematika yang kompleks selama 10 putaran (ronde) untuk menghasilkan data terenkripsi. [2] NIST mengadakan sebuah kompetisi untuk mencari algoritma block cipher yang paling aman dan handal, dan pemenangnya adalah AES yang kemudian dijadikan standar enkripsi.[5]

McDonald's TB Simatupang merupakan salah satu cabang restoran *fast food* McDonald's Indonesia yang terletak di Jl. Nangka Raya, RT.6/RW.5, Tj. Barat DKI Jakarta. Restoran ini menggunakan teknologi dalam menjalankan operasionalnya. Beberapa contoh data yang digunakan antara lain data keuangan, data bahan baku, dan informasi keanggotaan. Dokumen atau data ini tidak boleh dilihat atau dibuka oleh sembarang orang, hanya yang mempunyai hak akses saja yang boleh mengakses dokumen tersebut karena datanya bersifat rahasia. Namun di resto ini Tidak ada sistem yang menunjang keamanan data ini. Dimana pengamanan data masih dilakukan secara fisik. Hal ini akan mengakibatkan hilangnya dokumen digital rahasia dan hilangnya kepercayaan. Meningkatnya kebutuhan untuk melindungi data dan informasi mendorong penggunaan kriptografi sebagai solusi keamanan yang efektif. [6]

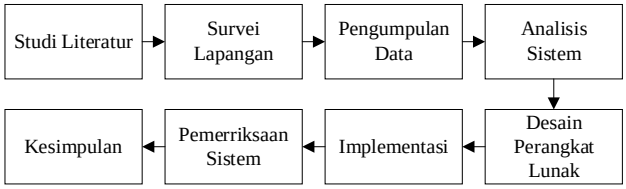
Saat ini belum ada mekanisme pengamanan untuk data tersebut, yang menyebabkan pernah terjadinya kebocoran data. Oleh karena itu, tujuan mengembangkan sebuah aplikasi web yang bertujuan untuk melindungi dan mengamankan isi data dokumen, serta mengurangi risiko penyalah gunaan data oleh pihak yang tidak bertanggung jawab. Salah satu metode yang digunakan adalah menerapkan algoritme kriptografi *Advanced Encryption Standard* (AES-128) yang terkenal karena keamanannya yang tinggi. Hal ini bertujuan untuk menjaga kerahasiaan dan keamanan data atau informasi penting yang disimpan dalam dokumen tersebut. [6]

Berdasarkan apa yang terjadi di atas, kontribusi penelitian ini adalah melakukan penelitian untuk mengamankan data yang ada di resto McDonald's TB Simatupang dalam penggunaan standar enkripsi lanjutan (AES-128). Dengan penjelasan tersebut bermaksud untuk mengembangkan aplikasi web dengan tujuan untuk melindungi data dan mencegah penyalahgunaan oleh pihak yang tidak bertanggung jawab. Guna tercapainya tujuan yang diinginkan, penggunaan metode algoritme *Advanced Encryption Standard* (AES-128) yang dikenal dengan tingkat keamanannya yang tinggi adalah solusi yang akan diterapkan. Dengan menggunakan algoritme ini, data akan diamankan dan hanya dapat dilihat oleh orang yang berwenang. [7]

II. METODE PENELITIAN

A. Metodologi Penelitian

Metodologi penelitian menjadi pedoman dalam melakukan penelitian untuk memastikan bahwa hasil yang diperoleh konsisten dengan tujuan yang telah ditetapkan sebelumnya. Tahapan implementasi metode penelitian yang digunakan dalam penelitian ini ditunjukkan pada Gambar 1 di bawah ini.



Gambar 1. Alur Metodologi Penelitian.

1. Studi Literatur

Metode penelitian yang melibatkan pengumpulan, analisis, dan sintesis informasi yang tersedia dalam berbagai sumber literatur untuk memperoleh pemahaman yang detil mengenai suatu topik atau masalah penelitian.

2. Survei Lapangan

Melibatkan pengumpulan data langsung dari lokasi atau populasi yang sedang diteliti.

3. Pengumpulan Data

Melalui wawancara dilakukan proses interaksi dengan seluruh pihak yang terlibat dalam pengembangan aplikasi dan program, dengan tujuan untuk memperoleh informasi mengenai aplikasi dan alat keamanan yang digunakan.

4. Analisa Sistem
   a. Analisis Data, merupakan tahap penting dalam menyelesaikan masalah keamanan. Pada tahap ini, dilakukan langkah-langkah yaitu melakukan pengumpuan fiel, bertujuan untuk mendapatkan data sebagai dasar untuk pembuatan program, mengelompokan fiel sesuai dengan jenis serta kegunaannya. Melakukan deskripsi data untuk menentukan tahapan yang diperlukan untuk membuat aplikasi yang mudah dipahami dengan tampilan yang baik.
   b. Analisa Penerapan Algoritme, Setelah mengumpulkan data yang diperlukan, langkah selanjutnya adalah menganalisis implementasi algoritme. Analisis implementasi algoritme mencakup langkah-langkah untuk menerapkan metode enkripsi Advanced Encryption Standard (AElS128) untuk melindungi data.
   c. Analisis Sistem, Proses penerapan kelamanan pada sistem meliputi langkah enkripsi fiel sebelum disimpan ke database. Enkripsi dipakai sebagai metode untuk pengamanan data yang terdapat di dalam database. Oleh karena itu, saat menyimpan data dalam database, harus menggunakan modul enkripsi yang diaktifkan saat pengguna mengakses dan melihat data. Modul kriptografi ini merupakan bagian dari aplikasi yang bertujuan untuk menjaga keamanan data di dalam sistem.

5. Desain Perangkat Lunak.

Pada tahap ini perancangan didasarkan pada hasil analisis sistem khususnya pada perancangan enkripsi dan dekripsi serta perancangan antarmuka. Metodologi air terjun tradisional digunakan untuk pelngelmbangan perangkat lunak. Model ini mengharuskan suatu fase diselesaikan secara menyeluruh sbelum melanjutkan ke fase berikutnya, dan hasil dari setiap fase harus di dokumentasikan dengan baik.

6. Implementasi

Tahap ini mengimplementasikan sistem secara terprogram dengan membangun aplikasi sesuai kebutuhan sistem berdasarkan rancangan sistem yang diterapkan. Pada tahap implementasi ini, modul-modul yang akan dibuat pada tahap desain diterjemahkan ke dalam kode bahasa pemrograman

tertentu. aplikasi berikut digunakan dalam konteks ini. Dalam penerapan pengamanan file data, perangkat lunak yang digunakan adalah bahasa pemrograman PHP dan DBMS dengan PhpMyAdmin. Perangkat keras yang digunakan adalah prosesor Intel Core i5, RAM 8GB, dan harddisk 1TB.

7. Pemeriksaan Sistem

Melalui pengujian black box, sistem diperiksa kesalahannya. Ketika dijalankan, aplikasi akan memastikan apakah input yang dimasukkan dan hasil yang diperoleh sudah benar.

8. Kesimpulan

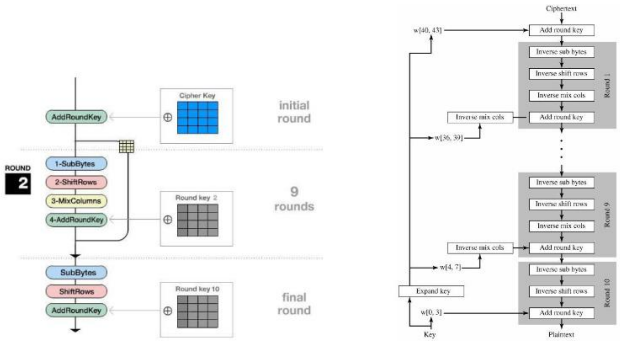
Kesimpulan pada fase ini, evaluasi akhir penerapan metode Advanced Encryption Standard (AES-128) untuk meningkatkan keamanan file telah dilakukan. Kesimpulan ini berdasarkan hasil pengujian yang dilakukan untuk mengevaluasi efektivitas penerapan metode Advanced Encryption Standard (AES) dalam menjaga keamanan file. Selain itu, saran perbaikan sistem dan pengembangan lebih lanjut juga akan disampaikan pada tahap ini untuk meningkatkan kualitas sistem.

B. *Advanced Encryption Standard*

Advanced Encryption Standard (AES) adalah sebuah algoritma enkripsi yang beroperasi pada blok data dengan panjang tertentu dan menggunakan kunci simetris untuk proses enkripsi maupun dekripsi. [7]Di tahun 2001, NIST (National Institute of Standard and Technology) menetapkan AES (Advanced Encryption Standard) sebagai standar algoritma kriptografi terbaru. Hal ini dilakukan untuk menggantikan DES (Data Encryption Standard) yang sudah tidak lagi aman dan masa penggunaannya telah berakhir. AES adalah algoritma enkripsi yang mampu mengamankan data dengan berbagai panjang kunci, yaitu 128 bit, 192 bit, dan 256 bit. Masing-masing panjang kunci menghasilkan jumlah putaran (round) enkripsi yang berbeda, seperti(Prameshwari & Sastra, 2018). [8]

C. Proses *Enkripsi*

Dalam proses enkripsi AES, terdapat empat transformasi dasar yang digunakan dengan urutan transformasi sebagai berikut: subbytes, shiftrows, mixcolumns, dan addroundkey. [9] Proses dekripsi menggunakan kebalikan dari setiap langkah transformasi dasar dalam AES, selain addroundkey. Urutan langkah-langkahnya adalah: invshiftrows, invsubbytes, addroundkey, dan invmixcolumns. Langkah awal dalam enkripsi data teks adalah mengubah teks menjadi kode ASCII, yang kemudian dikonversikan ke bilangan heksadesimal dan disusun menjadi matriks berukuran 4x4 yang berisi byte-byte data. Setelah konversi awal, teks yang dienkripsi mengalami serangkaian transformasi fundamental, yaitu subbytes, shiftrows, mixcolumns, dan addroundkey. Perlu diingat bahwa dalam setiap transformasi ini, data yang diolah adalah representasi biner dari matriks heksadesimal. Dengan ruang kunci sebesar 2^{128}, AES 128-bit menawarkan tingkat keamanan yang tinggi dan membuatnya sangat sulit, bahkan hampir mustahil, untuk dibobol melalui serangan brute force.



Gambar 2. Proses Enkripsi dan Dekripsi.

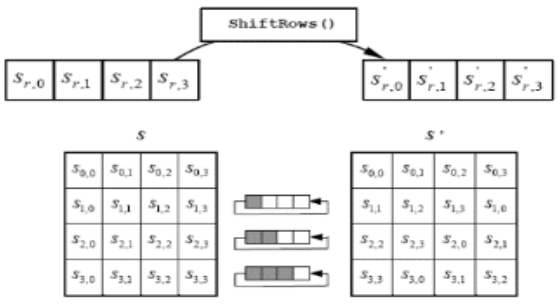
1. AddRoundKey, melakukan XOR antara keadaan awal (plainteks) menggunakan kunci enkripsi. Fase ini disebut juga initial *round*.

2. SubBytes, mempunyai Putaran sebanyak Nr – 1 kali. Proses yang dijalankan pada setiap putaran adalah: 1 *SubBytes*: substitusi *byte* menggunakan tabel substitusi (S-box). 2 ShiftRows: pergeseran baris-baris array state secara wrapping.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 3. Tabel S-box.[10]

3. ShiftRows adalah teknik yang menggeser elemen-elemen dalam setiap baris tabel atau blok. Baris pertama tidak digeser, sedangkan baris kedua digeser 1 byte ke kiri, baris ketiga digeser 2 byte ke kiri, dan seterusnya. Pergeseran ini terlihat seperti blok yang digeser ke kiri, dengan jumlah pergeseran tergantung pada jumlah byte yang diubah. Satu byte yang diubah berarti digeser 1 byte ke kiri. [9]



Gambar 4. *Shift Rows*

4. MixColumns, *MixColumns* digunakan untuk mengurutkan data secara acak di setiap kolom array state menggunakan

rumus berikut: A(x) = {03}x2 + {01}x2 + {01}x2 + {02} (1). [9]

5. Pada Algoritma AES, Key Expansion adalah proses yang mengubah kunci pengguna menjadi beberapa RoundKey. Jumlah RoundKey yang dihasilkan tergantung pada jumlah putaran (round) yang digunakan dalam enkripsi). [9]

D. Proses *Dekripsi*

Melnurut Ridwan Andriyanto, Khairijal, Delvit Satria Secara umum proses dekripsi AES-128 dengan kunci 128bit adalah sebagai berikut: [2]

1. InvShiftRows: Melakukan pergeseran baris dalam state ke kanan dengan jumlah tertentu
2. InSubBytes: Setiap elemen pada state dipetakan dengan tabel Inverse
3. InvMixColumns: Setiap kolom dalam state dikalikan dengan matriks AES.
4. AddRoundKey: Mengombinasikan state array dan round key dengan hubungan XOR.
5. Pada proses terakhir menghasilkan karakter teks asli (plaintext).

III. HASIL DAN PEMBAHASAN

Bagian ini membahas tentang implementasi algoritma AES-128 dalam sebuah aplikasi untuk enkripsi dan dekripsi data. Penjelasan meliputi flowchart, algoritma yang digunakan, proses enkripsi dan dekripsi, serta hasil dari enkripsi dan dekripsi dokumen.

A. *Flowchart* Menu Enkripsi

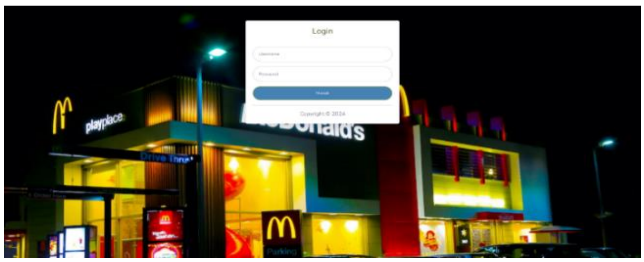
Berikut ini adalah flowchart enkripsi file. Dalam alur enkripsi file ini menjelaskan bagaimana proses enkripsi dilakukan pengguna dapat mengenkripsi file yang diinginkan lalu memasukkan password. Seteah itu program akan memproses dekripsi.

B. *Flowchart* Menu Dekripsi

Berikut ini adalah flowchart halaman dekripsi, alur flowchart ini menjelaskan proses penggunaan yang dapat di lakukan, pengguna dapat mengenkripsi file dan menghapus yang telah di enkripsi. Seteah memilih file harus memasukkan password, seteah itu program akan memproses enkripsi.

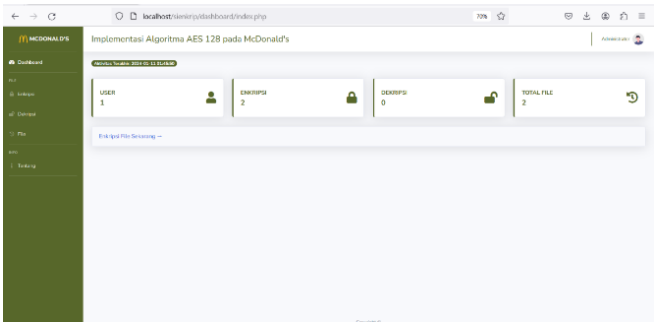
C. Tampilan Layar

Gambar 5 berikut menunjukkan antarmuka aplikasi pengamanan data, mulai dari menu login hingga menu logout.



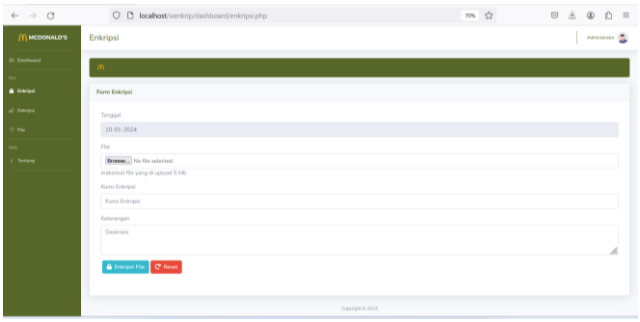
Gambar 5. Tampilan layar login

Halaman ini muncul pertama kali membuka *website*, berfungsi sebagai Halaman *login* sebelum masuk ke *dashboard*, user diwajibkan mengisi *username* dan *password* agar bisa masuk ke menu brikutnya.



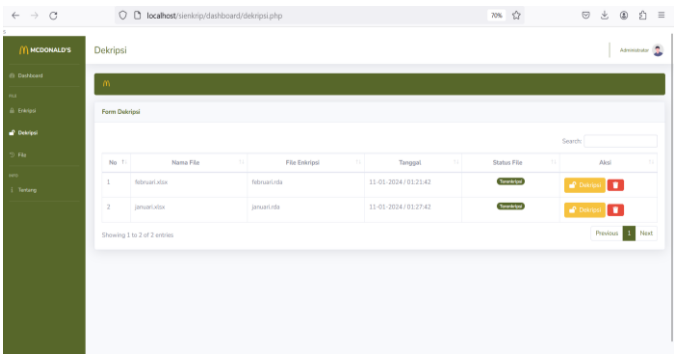
Gambar 6. Tampilam layar dashboard

Pada Tampilan layar *dasboard* ini terdapat beberapa side menu diantaranya, menu enkripsi, dekripsi, file, dan tentang, selain itu ada informasi aktifitas terakhir yang dilakukan user. pada menu *file* dapat melihat semua *file* yang telah di enkripsi dan di dekripsi lalu ada menu deskripsi sebagai informasi perusahaan.



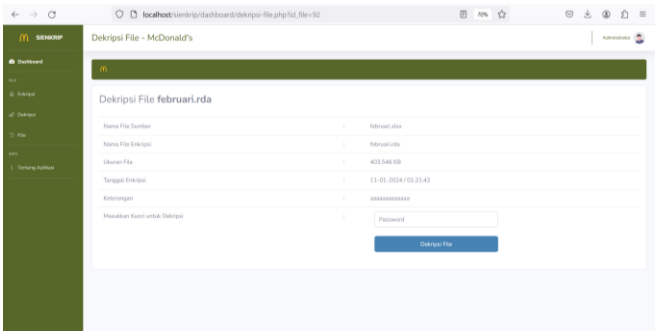
Gambar 7. Tampilan layar form enkripsi

Pada tampilan layar form aplikasi ini ada form tanggal pada form tersebut otomatis mengikuti tanggal disaat kita melakukan enkripsi tersebut, lalu ada form *password* yang wajib di isi user untuk mengamankan file dan form keterangan untuk memberi judul file hasil enkripsi. Form file berfungsi untuk memilih file yang ingin dienkripsi



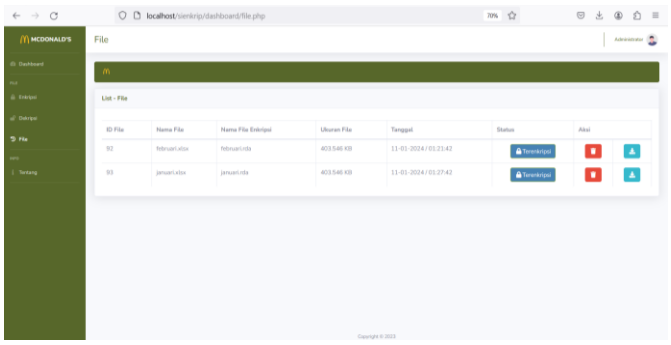
Gambar 8. Tampilan layar dekripsi

Halaman dekripsi menampilkan nama file-file asli yang telah dienkripsi, nama file enkripsi, tanggal enkripsi, status file merupakan informasi file yang sudah terenkripsi atau masih terdekripsi, dan di bagian aksi user bisa langusng melakukan hapus file atau melanjutkan proses dekripsi



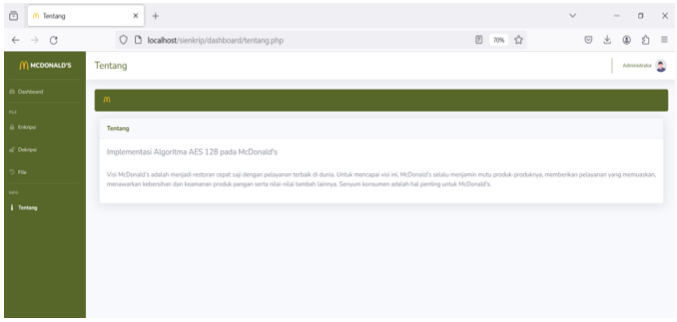
Gambar 9. Tampilan deskripsi file

Pada tampilan layar form dekripsi dalam aplikasi ini, tujuannya adalah untuk menampilkan sebuah tabel yang akan diisi ketika ada berkas sedang dalam proses enkripsi. Setelah berkas tersebut berhasil dienkripsi, akan muncul kolom tindakan "dekripsi berkas" sebelum melakukan dekripsi user terlebuh dahulu memasukan *password* yang di buat ketika melakukan enkripsi.



Gambar 10. Tampilan layar file

Halaman *File* merupakan halaman yang menampilkan daftar file yang telah dienkripsi dan didekripsi. Pada halaman ini, terdapat tombol unduh (download) untuk file yang telah dienkripsi dan didekripsi. Selain itu, pada daftar file juga terdapat tombol hapus (delete) untuk file yang telah dienkripsi dan didekripsi.



Gambar 11. Tampilan layar tentang

Pada halaman ini menampilkan tentang informasi perusahaan.

D. Pengujian

Pengujian menunjukkan dua aspek penting, yaitu kecepatan enkripsi dan hasil enkripsi berupa file yang tidak dapat dibuka. Selain itu, pengujian juga mengukur perubahan ukuran data sebelum dan sesudah dienkripsi menggunakan algoritma AES-128. Detail hasil pengujian dapat dilihat pada tabel 1 di bawah ini.

Tabel 1. Hasil Enkripsi

No	Dokumen	Ukuran asli dokumen	Ukuran dokumen hasil Enkripsi	Status	
				Enkripsi	Waktu
1	Update menu. pdf	137kb	136KB	Berhasil	3.28 detik
2	jan. xlsx	15kb	14.7959 KB	Berhasil	0.37 detik
3	feb. xlsx	15kb	14.8711 KB	Berhasil	0.4 detik
4	marc. xlsx	18kb	17.9863 KB	Berhasil	0.51 detik
5	Peserta Hygine Sanitasi. xlsx	32kb	31.543 KB	Berhasil	0.82 detik
6	Prosedur pemasakan. pdf	982kb	981.849 KB	Berhasil	21.71 detik
7	Resep 1. pdf	976kb	975.661 KB	Berhasil	23.71 detik
8	Resep 2. pdf	901kb	900.098 KB	Berhasil	23.85 detik
9	Selip gaji. docx	525kb	251.111 KB	Berhasil	6.01 detik

Tabel 2. Hasil Deskripsi

No	Dokumen	Ukuran asli dokumen	Ukuran dokumen hasil Enkripsi	Status	
				Enkripsi	Waktu
1	jan.xlsx	18kb	30.8828 KB	Berhasil	0.7 detik
2	feb. xlsx	27kb	26.8594 KB	Berhasil	0.66 detik
3	marc. xlsx	23kb	22.2988 KB	Berhasil	0.58 detik
4	april. xlsx	18kb	17.4658 KB	Berhasil	0.44 deltik
5	Prosedur pemasakan. pdf	29kb	28.8613 KB	Berhasil	0.94 detik
6	Peserta Hygine Sanitasi. xlsx	31kb	30.8828 KB	Berhasil	0.8 detik
7	Resep 2. pdf	27kb	26.9746 KB	Berhasil	0.68 detik
8	Resep 1. pdf	119kb	118.795 KB	Berhasil	2.95 detik
9	Peserta Hygine Sanitasi. xlsx	189kb	188.23 KB	Berhasil	2 detik

IV. KESIMPULAN

Berdasarkan uraian masalah pada bab sebelumnya dikembangkan dan dapat disimpulkan bahwa program aplikasi keamanan file berbasis web untuk McDonald's TB Simatupang menggunakan metode Advanced Encryption Standard (AES-128) adalah sebagai berikut:

1. Dari hasil pengujian yang dilakukan terlihat ukuran dokumen asli masih sama dengan ukuran yang telah di enkripsi
2. Aplikasi ini hanya dapat mengenkripsi dokumen yang berformat (*docx, *xlsx, *txt, *pdf, dan *ppt)
3. Aplikasi pengamanan *file* ini tidak merubah ukuran *file* asli yang dienkripsi

REFERENSI

[1] B. Saskia, D. Saputra, and M. Syafrullah, "3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 30 Agustus 2023-Jakarta," 2023.

[2] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA*, vol. 15, no. 1, pp.7-14, 2016, [Daring]. Tersedia pada: http://ejournal.unisba.ac.id

[3] R. Febrianto and S. Waluyo, "Implementasi Algoritme Kriptografi Advanced Encryption Standard (AES-256) Untuk Mengamankan Database Penilaian Karyawan Pada KJPP NDR," Bit (Fakultas Teknologi Informasi), vol. 20, no.1, pp. 44-49, 2023.

[4] W. Wieko, K. Adnan, E. P. Aprillia, and D. M. Iskandar, "Implementasi Pengamanan Akses Reporting Budget Dealer Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) Pada Microsoft Powerapps," *Journal of Information Technology and Computer Science (INTECOMS)*, vol. 7, no. 3, pp. 901-907, 2024.

[5] M. T. Rahman, A. Pinandito, and E. S. Pramukantoro, "Perbandingan Performansi Algoritme Kriptografi Advanced Encryption Standard (AES) dan Blowfish Pada Text di Platform Android," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 1, no. 12, pp. 1551-1559, 2017.

[6] R. Andriyanto, *et al.*, "Penerapan Kriptografi AES Class Untuk Pengamanan URL Website dari Serangan SQL INJECTION," *UNITEK*, vol. 13, no. 1, pp. 34-48, 2020.

[7] T. R. Syafutra, Khairil, and E. Suryana, "Penerapan Kriptografi Modern Pada Pengamanan Data Dokumen," *Jurnal Media Computer Science*, vol. 1, no. 2, pp. 287-294, 2022.

[8] A. Prameshwari dan N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 untuk Enkripsi dan Dekripsi File Dokumen," *Eksplora Informatika*, vol. 8, no. 1, pp. 52, 2018.

[9] N. W. Hidayatulloh, *et al*, "Mengenal Advance Encrytion Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data," *Digital Transformation Technology (Digitech)*, vol. 3, no. 1, pp. 1-10, 2023.

[10] M. M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," *Jurnal Pseudocode*, vol. 3, no. 2, pp. 129-136, 2016.