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

IMPLEMENTASI ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES-128) BERBASIS WEB PENGAMANAN DATA PADA MANJA JAKARTA

Muhammad Ragil Wicaksana[1*], Mufti[2]

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

Email: [1*]Ragilwicaksana10@gmail.com, [2]mufti@budiluhur.ac.id
(* : corresponding author)

Abstrak- Keamanan sebuah data menjadi hal yang penting untuk saat ini. Pentingnya menjaga data tranksaksi ini bertujuan untuk mencegah orang yang tidak berkepentingan mengubah data transaksi tersebut. Manja Jakarta belum memiliki kemananan data tranksaksi.Sebuah metode yang sering dipakai saat ini adalah kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik enkripsi text asli menjadi tersusun secara acak dan merubah teks menjadi sulit untuk dibaca. Tujuannya untuk tidak diketahui atau dimanfaatkan oleh yang tidak bekepentingan. Satu diantara metode algoritma kriptografi yang digunakan dalam penelitian ini adalah Advanced Encrypt Standar (AES-128). AES-128 merupakan algoritma chipper yang aman untuk melindugi data yang bersifat rahasia. AES-128 pertama kali diperkenalkan pada tahun 2001 oleh *NIST (National Institusi of Standar and Technology)* untuk menggantikan algoritma DES. tujuan dari peneliatian ini untuk meningkatkan keamanan pada Manja jakarta dengan mengimplementasikan kriptografi Advanced Standard Encrypt (AES-128). Hasil *file* yang telah ternkripsi aplikasi Kriptografi AES-128 berbasis web yang dibuat oleh peneliti tidak dapat terbaca dan tidak dapat dimanfaatkan oleh yang tidak berkepentingan. Tampilan website program kriptografi AES-128 yang dibuat dengan sederhana sehingga mudah dipahami dan kekurangan dari aplikasi yang dibuat hanya dapat memproses format file berupa .word, .pdf, ,xlxs. Dan dengan adanya aplikasi kriptografi AES-128 diharapkan dapat meningkatkan keamanan data pada Manja Jakarta.

Kata kunci : Kriprografi, AES-128, Data

WEB-BASED IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD (AES-128) ALGORITHM FOR DATA SECURITY AT MANJA JAKARTA

Abstract- *Data security has become increasingly important today. The importance of protecting transaction data is to prevent unauthorized individuals from altering it. Manja Jakarta currently lacks adequate transaction data security. A commonly used method for securing data is cryptography. Cryptography is the science of studying techniques to encrypt original text into a scrambled* format, *making it difficult to read. The goal is to ensure that the data remains unknown and unusable by unauthorized parties. One of the cryptographic algorithms used in this research is the ADVANCED ENCRYPTION STANDARD (AES-128). AES-128 is a secure cipher algorithm used to protect sensitive data. It was first introduced in 2001 by the National Institute of Standards and Technology (NIST) to replace the DES algorithm. The purpose of this research is to enhance security at Manja Jakarta by implementing the ADVANCED ENCRYPTION STANDARD (AES-128) cryptography. The files encrypted using the web-based AES-128 cryptography application developed by the researcher cannot be read or utilized by unauthorized individuals. The AES-128 cryptography program's website interface was designed to be simple and easy to understand, with the limitation that it can only process file* formats *such as .docx, .pdf, and .xlsx. It is hoped that the implementation of AES-128 cryptography will improve data security at Manja Jakarta.*

Keywords: Cryptography, AES-128, Data

1. PENDAHULUAN

Manja Jakarta adalah Perusahaan yang bergerak dalam jasa pelayanan percetakan kalender dan spanduk sesuai dengan kebutuhan kantoran lainnya ditunjang dengan peralatan-peralatan canggih yang memadai dan didukung dengan unit unit bisnis lain untuk memenuhi kebutuhan pelanggan yang sangat beragam. informasi tersebut masih dalam file yang disimpan secara umum dalam format *pdf dan *xlsx, yang dapat diakses oleh pengguna yang tidak berwenang. Sementara itu, data dari Percetakan hanya dapat diakses oleh manajer dan anggota staf dari Manja Jakarta.

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Manja Jakarta belum memiliki keamanan terhadap data transaksi penjualan tersebut, karena percetakkan tersebut menerima cukup banyak pesanan secara online dari beberapa perusahaan yang menyebabkan timbulnya kebocoran data transaksi penjualan dari pihak lain seperti kejahatan pengubah data penjualan. Untuk itu, sangat penting untuk memperhatikan keamanan data pengguna dalam pengembangan aplikasi[1]. Oleh karena itu, sistem berbasis keamanan jaringan komputer (*cyber security*) kini telah dikembangkan. Salah satu metode yang sering digunakan saat ini adalah *cryptography* [2].

Pada penelitian sebelumnya yang dilakukan oleh Joko Handoyo pada tahun 2020 yang berjudul "Keamanan dokumen menggunakan *Algoritma ADVANCED ENCRYPTION STANDARD (AES)* Studi ini menekankan pentingnya keamanan data dalam era teknologi, terutama dalam konteks pengamanan *file* dokumen atau data. Kriptografi menjadi solusi, dengan fokus pada konsep enkripsi dan dekripsi. Dan memiliki tujuan untuk mengamankan dokumen dengan menggunakan algoritma AES. Dengan konsep enkripsi *file* yang awalnya terbaca menjadi tidak terbaca dan melalui konsep dekripsi *file* yang awalnya enkripsi dapat terbaca kembali[3].

Lalu pada penelitian Ricaro Laila pada tahun 2020 yang berjudul "Implementasi Algoritma AES-256 dan LSB pengamanan dan penyisipan pesan *Teks* dan pada *Audio"* pada Penelitian ini berfokus pada pentingnya pengamanan informasi multimedia seperti foto, video, gambar bergerak, dan audio dalam bentuk MP3, terutama untuk melindungi data yang bersifat rahasia dari pembajakan dan penyebaran yang tidak diinginkan. Solusi dari masalah ini ialah dengan adanya kriptografi yang digunakan sebagai metode pengamanan informasi, khususnya melalui algoritma *ADVANCED ENCRYPTION STANDARD* (AES). Tujuan dari penelitian ini juga untuk menggabungkan kekuatan kriptografi AES dengan metode steganografi LSB untuk mengamankan informasi multimedia, khususnya file audio suara, sehingga dapat menjaga kerahasiaan dan integritas data dari ancaman pihak yang tidak berwenang.[4]

Adapun rumusan masalah berdasarkan latar belakang yang telah dibahas yaitu Bagaimana cara untuk mengamankan file dan Bagaimana cara *Advanced Encrypt Standart* (AES) 128 untuk mengamankan file? Oleh karena itu, tujuan dari penulisan ini adalah untuk meningkatkan keamanan data dan membantu mengatasi kebocoran data pada Manja Jakarta dengan mengimplementasikan kriptografi AES-128.

2. METODE PENELITIAN

2.1 Penerapan Metode

Pada gambar 1 merupakan proses yang dijalankan oleh peneliti dalam penerapan metode.

Gambar 1. Penerapan Metode

a. Studi Literatur, Pada tahap Studi literatur dilakukan dengan mempelajari konsep *ADVANCED ENCRYPTION STANDARD* (AES-128).
b. Studi Lapangan, Pada tahap ini dilakukan pengamatan langsung pada Manja Jakarta. tujuannya untuk mengidentifikasi Masalah yang ada pada Manja Jakarta
c. Perumusan Masalah, Bagaimana cara mengamankan Data Manja Jakarta menggunakan Kriptografi AES 128 ?
d. Pengumpulan Data, mengumpulkan data pada Manja Jakarta untuk memperoleh dokumen yang perlu diamankan.
e. Analisis Sistem, Analisis masalah perlu dilakukan untuk persiapan apa saja kebutuhan aplikasi pengamanan data dengan metode AES 128 bit
f. Perancangan Sistem, Dalam tahap ini, hasil analisis sistem digunakan untuk mengarahkan proses desain, dengan fokus pada modul yang menangani enkripsi dan dekripsi serta komponen tambahan lainnya yang

akan diintegrasikan ke dalam aplikasi. Selanjutnya, desain antarmuka dilakukan untuk memastikan keselarasan sistem.

g. Implementasi, Pada tahap ini untuk mengimplementasi aplikasi yang digunakan pada *hardware* menggunakan processor *Intel Core i5-83350u,* memory 12 GB DDR4-RAM, dan penyimpanan 240GB M 2 SSD, dan pada *Software* menggunakan Windos 10 Pro, Aplikasi yang digunakan *Visual Studio Code, Xampp, Google*

h. Pengujian Sistem, Pada tahap pengujian ini, dilakukan untuk memastikan bahwa sistem yang telah dibangun sesuai dengan hasil analisis dan perancangan, serta untuk mengevaluasi apakah sistem tersebut memenuhi harapan berdasarkan masalah dan tujuan yang telah ditetapkan. Adapun pengujian yang akan dilakukan pada algoritma enkripsi *ADVANCED ENCRYPTION STANDARD (*AES-128) berupa kecepatan waktu dalam memproses enkripsi *file* dan kecepatan waktu dalam memproses dekripsi *file* dan hasil nama format *file* yang telah melalui enkripsi maupun dekripsi.

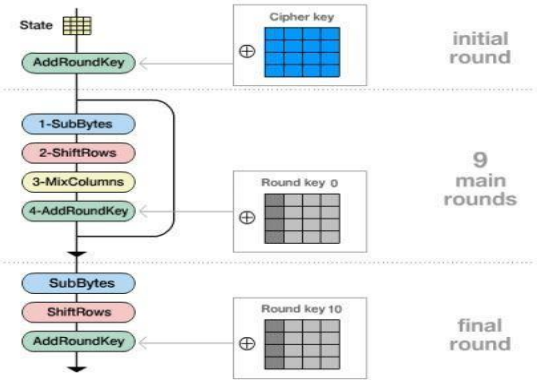
2.2 Kriptografi

Kriptografi merupakan ilmu yang mempelajari cara untuk mengamankan yang berhubungan dengan aspek keamanan informasi seperti antektikasi, kerahasiaan data, keabsahan data dan data integritas[5]. *Cryptography* yang berasal dari bahasa Yunani,terdiri dari kata "*crypto*" dan "*graphia*" yang mempunyai arti yaitu penulisan rahasia[6],[7]. Dengan cara ini, pengguna yang tidak berwenang tidak bisa mengakses informasi asli dari data tersebut, sehingga dapat mencegah penyalahgunaan data [8].

2.3 Algoritma *Advanced Encprytion Standart* (AES-128)

2.3.1 Proses Enkripsi Algoritma *ADVANCED ENCRYPTION STANDARD*

Pada proses awal enkripsi AES-128 dimana teks asli dibentuk menjadi *State*. setelah itu mengkonversi nya ke dalam bentuk heksadesimal dengan melihat tabel KODE ASCII. Kemudian sebelum memulai *round* 1 heksadesimal pada teks asli digabungkan dengan kunci *round* ke 0 (transformasi ini disebut dengan *AddRoundKey*). Kemudian melanjutkan *round* 1 sampai dengan *round* 10 Setiap *round* menggunakan 4 jenis transformasi sebagai Gambar 2 berikut.

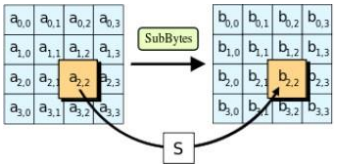


Gambar 2. Proses Enkripsi Algoritma AES

a. *Transformation Subbytes*, Hasil setiap *round* disubtitusikan sesuai tabel *s-box* Gambar 3 dengan ilustrasi Gambar 4.

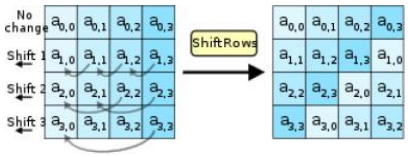
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Gambar 3. Tabel *S-Box*



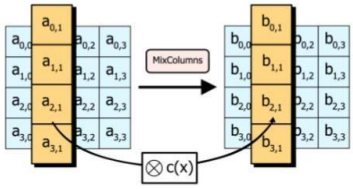
Gambar 4. Transformasi *Subbytes*

b. Transformasi *Shiftrows*, Hasil dari *SubBytes* mengalami pergeseran. dimana pada Gambar 5 baris 1 tidak mengalami pergerseran, pada baris ke 2 mengalami pergeseran 1 kolom, baris 3 mengalami pergeseran 2 kolom, dan baris ke 4 mengalami pergeseran 3 kolom.



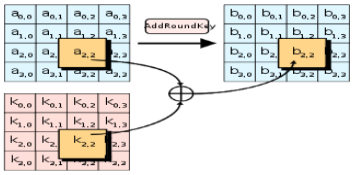
Gambar 5. Transformasi *Shiftrows*

c. Transformasi *Mixcolumn*, pada Gambar 6 hasil dari *ShiftRows* dikalikan dengan matriks yang sudah ditetapkan.



Gambar 6. Transformasi *Mixcolumn*

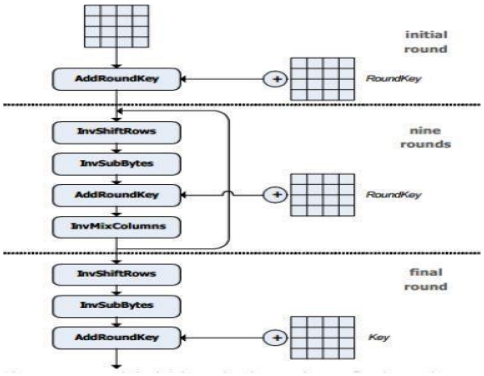
d. Transformasi *Add Round Key*, Pada Gambar 7 hasil dari *MixColumns* digabungkan dengan hasil pada setiap *round*.



Gambar 7. Transformasi *Add Roundkey*[9]

2.3.2 Proses Dekripsi Algoritma *ADVANCED ENCRYPTION STANDARD*

Pada proses deskripsi AES-128, merupakan kebalikan dengan proses enkripsi. Pada proses deskripsi Gambar 8 menggunakan 4 transformasi *invers* diantaranya *InvSubBytes, InvShiftRows, InvMixColoumns*, dan *AddRoundKey*. Proses Dekripsi AES-128 memiliki perbedaan dalam proses pengerjaannya, pada deskripsi dimulai mencari hasil dari setiap *round* kemudian hasil dari setiap *round* di tran*form*asikan *InvShiftRows, InvSubBytes*, *AddRoundKey* dan terakhir *InvMixColoumns*. dan Pada *round* ke 10 hanya melakukan 3 proses transformasi tanpa melalui transformasi *InvMixColoumns.*

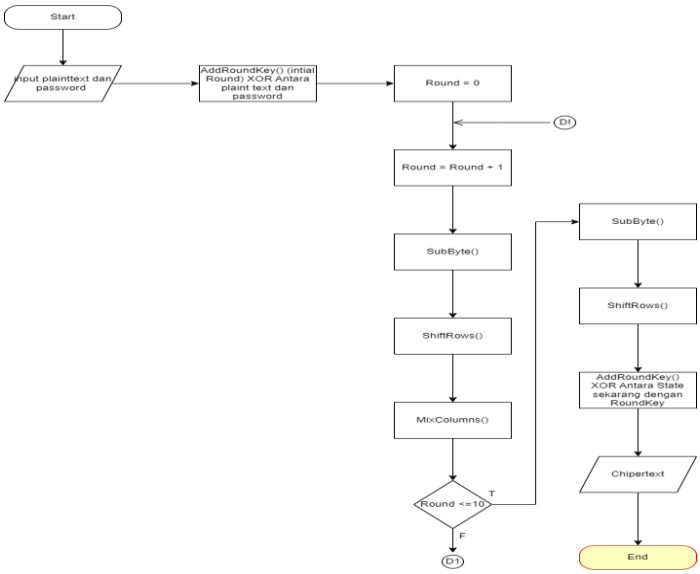


Gambar 8. Ilustrasi Proses Dekripsi AES[10]

3. HASIL DAN PEMBAHASAN

3.1 *Flowchart* Enkripsi

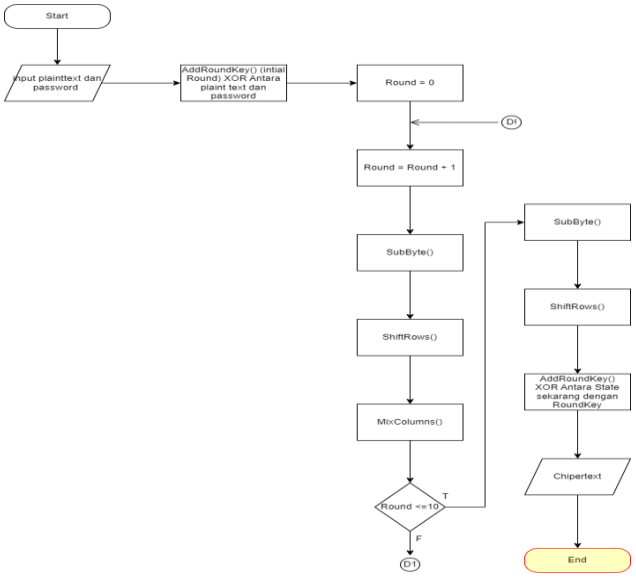
Flowchart Gambar 9 dari proses enkripsi file menggunakan AES-128. Proses dimulai dengan simbol *start*, diikuti dengan memasukkan *plaintext* dan kunci (*key*). Komputer kemudian menggabungkan *plaintext* dengan kunci. Selanjutnya, komputer menjalankan proses enkripsi melalui 10 putaran (*rounds*). Pada setiap putaran, komputer melakukan transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Namun, pada putaran ke-10, hanya *SubBytes*, *ShiftRows*, dan *AddRoundKey* yang diproses. Proses ini menghasilkan *ciphertext* dan diakhiri dengan simbol *end*.



Gambar 9. *Flowchart* Enkripsi AES-128

3.2 *Flowchart* Dekripsi

Flowchart dari proses dekripsi *AES-128*. Proses Gambar 10 dimulai dengan simbol *Start*, diikuti dengan memasukkan *ciphertext* dan kata sandi (*password*). Komputer kemudian menggabungkan *ciphertext* dan kata sandi sebelum *round* 0. Selanjutnya, komputer memproses dari *round* 1 hingga *round* 10, di mana pada setiap *round*, sistem akan menjalankan *InvShiftRows*, *InvSubBytes*, *AddRoundKey*, dan *InvMixColumns*. Pada *round* 10, jika terjadi kesalahan, proses akan diulang dari *round* 1. Jika benar, komputer melanjutkan dengan memproses *InvShiftRows*, *InvSubBytes*, dan *AddRoundKey* untuk menghasilkan *plaintext*. *Flowchart* ini diakhiri dengan simbol *End*.



Gambar 10. *Flowchart* Dekripsi AES-128

3.3 Tabel Pengujian

Pada tabel 1 dan tabel 2 pengujian ini merupakan hasil dari penelitian pengujian untuk melakukan perbandingan antara proses enkripsi *file* dan proses dekripsi *file*. Pengujiannya terdiri dari format file, ukuran *file*, waktu untuk melakukan proses enkripsi, dan waktu proses dekripsi.

3.3.1 Pengujian Proses Enkripsi

Tabel 1. Pengujian Proses Enkripsi

No	Nama Dokumen	Format File	Ukuran File (KB)	Waktu Enkripsi (Detik)	Ukuran Hasil Enkripsi (KB)	Nama File Hasil Enkripsi
1	Faktur Iskandar	XLSX	32	3.47	32	96287-faktur-iskandar
2	Invoice manja	XLSX	329	11.93	329	82619-invoice-manja
3	PO Febuari	XLSX	243	9.20	243	55252-po-febuari-2024
4	PO Maret	XLSX	1	6.87	182	23946-po-maret
5	PO April	XLSX	183	6.75	183	25463-po-april

3.3.2 Pengujian Proses Dekripsi

Tabel 2. Pengujian Proses Dekripsi

No	Nama Dokumen	Format File	Ukuran File (KB)	Waktu Dekripsi (Detik)	Ukuran Hasil Dekripsi (KB)	Nama File Hasil Dekripsi
1	96287-faktur-iskandar	RDA	32	1.69	32	51044-faktur-iskandar
2	82619-invoice-manja	RDA	329	11.87	329	81686-invoice-manja
3	55252-po-febuari-2024	RDA	243	8.94	243	58319-po-febuari-2024
4	23946-po-maret	RDA	182	6.85	182	65951-po-maret
5	25463-po-april	RDA	183	6.10	183	84556-po-april

Berdasarkan dengan hasil pengujian yang dilakukan terhadap program, untuk format file yang diuji yaitu .xlxs, .pdf. Hasil pengujian program yang dijalankan mengungkapkan beberapa kelebihan dan kelemahan aplikasi ini :

3.3.3 Kelebihan Dari Aplikasi

a. Tampilan *Website* yang dibuat mudah dipahami.
b. *File* yang telah terenkripsi tidak dapat di baca sebelum melalui proses dekripsi.
c. Dekripsi file tidak dapat dilakukan sebelum memasukkan key pada proses enkripsi.
d. Setelah melakukan proses enkripsi menghasilkan format file yang berbeda.
e. File yang telah terenkripsi terdapat *magic number* pada awal file yang telah terenkripsi.

3.3.4 Kelemahan Dari Aplikasi

a. Kecepatan enkripsi dan dekripsi file tergantung pada ukuran file. Semakin kecil ukuran file, semakin cepat proses enkripsi dan dekripsi dilakukan.
b. Format file yang dapat dilakukan proses enkripsi dan dekripsi hanya berupa .xlxs, .pdf, .word belum bisa menenkripsi format video, gambar dan audio.
c. Tampilan pada aplikasi sederhana.
d. Hasil dari proses enkripsi hanya dapat dibuka dengan aplikasi notepad.

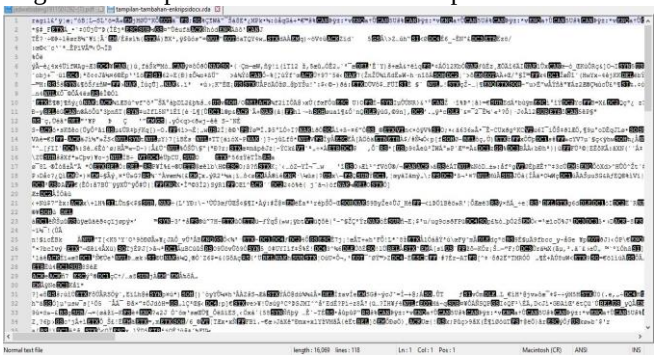
3.4 Tampilan Layar

3.4.1 Tampilan Layar Halaman Enkripsi

Pada halaman Gambar 11 enkripsi ini untuk melakukan proses enkripsi pada aplikasi yang dibuat. pengguna menginput file yang ingin di enkripsi yang Memiliki format file .pdf, .docx, .xlsx, .txt dan .pptx. Jika memasukkan format file yang tidak sesuai maka aplikasi menampilakan pesan Maaf, file yang bisa dienkrip hanya word, excel, text, ppt ataupun pdf.. Kemudian masukkan *password* dan deskripsi untuk mengamankan file tersebut. Berikut tampilan halaman enkripsi.

Gambar 11. Tampilan Layar Halaman Enkripsi

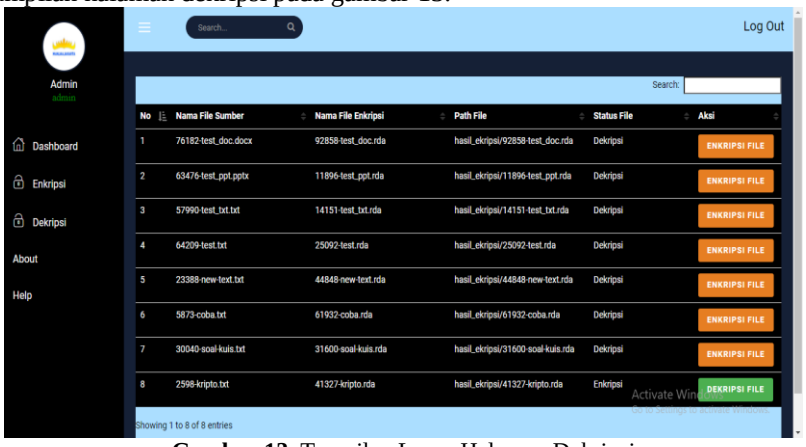
Berikut Gambar 12 hasil file dari proses enkripsi file yang sudah dimasukkan pada *form*. Pada hasil file proses enkripsi terdapat *Magic Number*/Kode pada awal file. Berfungsi ungtuk keamanan tambahan sehingga pihak yang tidak berkepentingan tidak dapat memalsukan data enkripsi



Gambar 12. Hasil Proses Enkripsi File

3.4.2 Tampilan Layar Halaman Dekripsi

Pada tampilan ini menampilkan daftar file yang dienkripsi dan file didekripsi. Pada tampilan halaman deskripsi terdapat tombol aksi, ketika pengguna menekan tombol aksi enkripsi file maka pengguna dialihkan ke halaman enkripsi, dan saat pengguna menekan aksi dekripsi file maka pengguna dialihkan ke halaman *form* dekripsi. Berikut tampilan halaman dekripsi pada gambar 13.



Gambar 13. Tampilan Layar Halaman Dekripsi

3.4.3 Tampilan Layar Halaman *Form* Dekripsi

Pada halaman *form* dekrispi ini lanjutan dari halaman dekripsi, pada halaman ini berfungsi untuk mengubah file yang telah terenkripsi. Agar file tersebut bisa berubah, pengguna perlu memasukkan *key* yang sama pada saat melakukan enkripsi tersebut. Berikut *form* dekripsi pada gambar 14.

Gambar 14. Tampilan Layar Halaman *Form* Dekripsi

4. KESIMPULAN

Peneliti menyimpulkan bahwa penggunaan program kriptografi AES-128 dapat melindungi data transaksi pada Manja Jakarta dengan baik, karena file yang telah terenkripsi tidak dapat dibaca sebelum proses dekripsi dilakukan. Selain itu, kecepatan enkripsi dan dekripsi file sangat dipengaruhi oleh ukuran file; semakin kecil ukuran file, semakin cepat proses enkripsi dan dekripsi berlangsung. Adapun saran dari peneliti untuk pengembangan aplikasi agar menjadi lebih baik lagi antara lain: diharapkan ke depannya aplikasi dapat menambahkan dukungan untuk berbagai format file dalam proses enkripsi dan dekripsi, serta mengembangkan versi mobile atau Android agar aplikasi lebih mudah diakses dan digunakan di berbagai perangkat. Selain itu, aplikasi diharapkan dapat dikembangkan dengan menggunakan dua metode kriptografi untuk meningkatkan keamanan file.

DAFTAR PUSTAKA

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

[2] N. Chafid and H. Soffiana, "Impelementasi Algoritma Kriptografi Klasik Caesar Untuk Rancang Bangun Aplikasi E-Voting Berbasis Web (Studi Kasus : Sman 10 Tangerang)," *J. Ilm. Sains dan Teknol.*, vol. 6, no. 2, pp. 133–145, 2022, doi: 10.47080/saintek.v6i2.2249.

[3] J. Handoyo and Y. M. Subakti, "Keamanan Dokumen Menggunakan Algoritma ADVANCED ENCRYPTION STANDARD (Aes)," *J. SITECH Sist. Inf. dan Teknol.*, vol. 3, no. 2, pp. 143–152, 2020, doi: 10.24176/sitech.v3i2.5865.

[4] R. Laia, "Implementasi Algoritma Aes 256 Bit Dan Lsb Untik Pengamanan Dan Penyisipan Pesan Teks Pada File Audio," *Pelita Inform. Inf. dan Inform.*, vol. 8, no. April, pp. 467–469, 2020, [Online]. Available: https://www.ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/2445

[5] Widyawan, Dian, and Imelda 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.

[6] 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," *Digit. Transform. Technol.*, vol. Vol.03, no. No.1, pp. 1–10, 2023, [Online]. Available: https://jurnal.itscience.org/index.php/digitech/article/view/2293

[7] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," KOMIK (Konferensi …, vol. 4, pp. 78–86, 2020, doi: 10.30865/komik.v4i1.2590.

[8] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *J. Comput. Syst. Informatics*, vol. 4, no. 1, pp. 179–187, 2022, doi: 10.47065/josyc.v4i1.2451.

[9] G. C. M. Purba and A. ID Hadiana, "Pengamanan Citra Medis Berbasis Steganografi d an Kriptografi Dengan Menggunakan Metode End Of File Dan Advanced Encryption Standard," *Informatics Digit. Expert*, vol. 4, no. 1, pp. 1–9, 2022, doi: 10.36423/index.v4i1.878.

[10] A. Teguh Utomo and R. Pradana, "Implementasi Algoritma ADVANCED ENCRYPTION STANDARD (AES-128) Untuk Enkripsi dan Dekripsi File," Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia, no. September, pp. 21–23, 2022.