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

PENERAPAN ALGORITME *ADVANCED ENCRYPTION STANDARD* (AES-128) UNTUK MENGAMANKAN *FILE* DOKUMEN DI TOKO KAYU JATI NADIA

Bhagaswara Suwardana[1*], Mufti[2], Siswanto[3], Subandi[4]

[1,2,3,4]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta , Indonesia

Email: [1]1911500773@student.budiluhur.ac.id, [2]mufti_hayat@yahoo.com, [3]siswanto@budiluhur.ac.id, [4]subandi@budiluhur.ac.id
(* : corresponding author)

Abstrak-Hasil penelitian ini memberikan manfaat yang signifikan bagi instansi Toko Kayu Jati Nadia. Penelitian ini memberikan solusi yang efektif dalam meningkatkan keamanan *file-file* penting yang disimpan dalam bentuk *excel* dan *word.* Masalah yang sering terjadi adalah kehilangan data hingga berubah nya data pada instansi Toko Kayu Jati Nadia, sehingga dari permasalahan inilah terjadinya penelitian terhadap kebocoran data dibuat, dengan menggunakan aplikasi Kriptografi yang diterapkan algoritme AES-128. Hasil pengujian keamanan *file* menunjukkan bahwa penerapan algoritme AES-128 dapat berhasil dilakukan secara efisien di berbagai konteks lainnya, selama digunakan dengan tepat dan bertanggung jawab, meningkatkan keamanan data di berbagai sektor. Masalah yang sering terjadi dalam toko nadia adalah *file* atau dokumen data didalam toko terkadang mengalami kehilangan atau *file* tersebut terkadang mengalami perubahan tanpa sepengetahuan pemilik. Karena pengamanan data pelanggan sangat penting maka diperlukannya sistem keamanan untuk *file.* Dalam penelitian ini, Toko Kayu Jati Nadia memiliki data arsip yang sangat penting dan harus dijaga keamanannya dengan baik. Saat ini, file-file tersebut disimpan tanpa langkah-langkah pengamanan yang memadai, baik dalam *folder* komputer maupun *flash disk.* Oleh karena itu, penelitian ini bertujuan untuk membuat sebuah aplikasi keamanan *file* berbasis web yang menggunakan algoritme kriptografi untuk melindungi dan mengamankan data arsip tersebut.Dalam aplikasi keamanan *file* ini, Akan ada perubahan pada isi *file* agar menjadi tidak terbaca dengan proses enkripsi, dan kemudian dapat dikembalikan ke keadaan semula agar dapat terbaca lagi melalui proses dekripsis. Dengan pengamanan isi *file* menggunakan teknik *Advanced Encryption Standard* (AES-128), Karena AES-128 tingkat keamanan nya tinggi dalam melindungi informasi saat pertukaran data. Dalam penggunaan aplikasi keamanan berbasis web ini. Toko Kayu Jati Nadia dapat memastikan jika data yang disimpan nya terjaga keamanannya dengan bagus. Proses enkripsi ini akan menjaga data dari akses data yang enggan diizinkan, sementara didalam proses dekripsi akan memungkinkan pengguna tersebut memiliki otorisasi untuk dengan mudah dan aman mengakses kembali *file* tersebut. Hasil akhir dari proses pengujian *file* rata-rata besar ukuran hasil enkripsi *file* adalah 18.445 *bytes*, kemudian rata-rata waktu pemrosesan enkripsi adalah 583 milidetik. Lalu ada hasil akhir dari proses rata-rata ukuran hasil besar *file* dekripsi adalah 18.445 *bytes* dan rata-rata waktu pemrosesan dekripsi adalah 503 milidetik.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, *File, Advanced Encryption Standard* (AES-128).

IMPLEMENTATION OF THE ADVANCED ENCRYPTION STANDARD (AES-128) ALGORITHM FOR DOCUMENT FILE SECURITY AT TOKO KAYU JATI NADIA.

Abstract-The results of this study provide significant benefits for related agencies. This research provides an effective solution in increasing the security of important files stored. In addition, this research also contributes to the development of knowledge and understanding of cryptographic algorithms, which can be a reference for further research in the field of file security using cryptographic algorithms. With the tests carried out on the file security system, the use of the AES-128 algorithm can be implemented effectively in various other fields with proper and responsible use. The problem that often occurs in Nadia stores is that data files or documents in the store are sometimes lost or these files are sometimes changed without the owner's knowledge. Because securing customer data is very important, a security system is needed for files. Nadia Teak Wood Store has various important archival data that needs to be kept safe. Currently, these files are still stored in computer folders or flash disks without adequate security. In this research, a file security application design will be made by modifying the contents of the file so that it cannot be read (encryption) and then can be returned to readability (decryption) through the implementation of a web-based file security application using a cryptographic algorithm. The method used to secure files is the Advanced Encryption Standard (AES-128). AES was chosen because it has a good level of

security in exchanging information. By implementing this file security application, Toko Kayu Jati Nadia can ensure that their archival data is well protected. The encryption process will protect data from unauthorized access, while the decryption process provides an opportunity for authorized users to access files again. The final result of the testing process is that the average size of the encrypted file is 18,445 bytes, then the average encryption processing time is 583 milliseconds. Then there is the end result of the process, the average size of the resulting decryption file is 18,445 bytes and the average decryption processing time is 503 milliseconds.

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

1. PENDAHULUAN

Pertumbuhan teknologi informasi berdampak besar pada kehidupan manusia. Namun, semakin luasnya penggunaan internet meningkatkan risiko penyadapan dan perang siber. [1]Kemampuan *cyber intelligence* penting untuk kemajuan bangsa Indonesia, terutama karena Indonesia menduduki peringkat tertinggi perang siber. Keamanan dan kerahasiaan data menjadi krusial untuk menjaga kemajuan bangsa ini.[2]

Kriptografi adalah sebuah ilmu serta seni yang berfungsi untuk menjaga tingkat keamanan pesan. Selain itu, kriptografi juga mampu mempelajari teknik-teknik matematika yang dapat berhubungan dengan aspek tingkat keamanan informasi, seperti kerahasiaan data, integritas data, dan otentikasi. Didalam pengertian tersebut, istilah "seni" mengacu pada metode berbeda untuk menyembunyikan pesan, sementara kata "*graphy*" dalam "*cryptography*" sendiri mengandung arti bahwa ini sudah mencerminkan sebuah seni.[3] Masalah yang sering terjadi pada belakangan terakhir ini adalah tentang kebocoran sebuah data , karena itulah pentingnya untuk mengamankan data dan pada permasalahan ini dibuatlah sebuah aplikasi untuk menyembunyikan data agar tidak bisa digunakan oleh orang yang tidak berwenang.[4] Tujuan dari penelitian ini adalah untuk Meminimalisir pengungkapan data/*file* penting dalam Toko Kayu Jati Nadia, dan Manfaat untuk instansi, bahwa hasil penelitian ini dapat menyediakan keamanan yang baik untuk *file-file* penting yang disimpan, dan juga memberikan pengetahuan dan edukasi baru mengenai algoritme kriptografi ini.

AES (*Advanced Encryption Standard*) termasuk dalam kategori kriptografi *key* satu arah (simetris) modern, di mana pada algoritma ini perlu menggunakan *key* yang identik untuk kedua proses *encrypt* dan *decrypt*.[5] Dengan menggunakan kunci yang sama, Data yang telah dienkripsi akan sangat sulit dipahami dan dimengerti oleh orang yang tidak punya akses ke kunci tersebut. Algoritma ini beroperasi dengan mengubah data ke dalam bentuk kode-kode khusus, sehingga informasi yang tersimpan tidak dapat dibaca oleh siapapun kecuali oleh orang-orang yang berhak memiliki kunci untuk mendekripsinya.[6]

Toko Kayu Jati Nadia merupakan sebuah bisnis kayu jati di wilayah Tangerang Selatan yang melayani pemesanan melalui *platform* online. Toko tersebut berlokasi di wilayah Pondok Kacang Timur, Tangerang Selatan. Toko tersebut menyimpan dokumen penting, termasuk data penjualan bulanan yang merupakan informasi rahasia, Tentang aspek positif dan negatif dari toko yang mungkin tidak diketahui oleh orang lain. Sayangnya, toko ini hanya mencatat penjualan melalui aplikasi *Microsoft Excel* yang rentan terhadap potensi peretasan data seperti kejahatan pengubahan data penjualan oleh oknum yang tidak berwewenang. Hal ini bisa menyebabkan kerugian bagi pemilik usaha Toko Kayu Jati Nadia.Oleh karena itu, diperlukan langkah-langkah untuk melindungi informasi penjualan tersebut agar tidak disalahgunakan oleh pihak yang tidak berwenang. Dalam rangka mengatasi tantangan tersebut, atau sebagai solusi atas masalah tersebut, muncul ide untuk Merencanakan suatu sistem keamanan yang memanfaatkan, atau mendesain sistem keamanan yang mengadopsi metode kriptografi AES-128 untuk menjaga keamanan data dalam *format file*.[7] Algoritma Pemilihan kriptografi AES-128 didasarkan pada kemampuannya untuk beroperasi dengan blok 128-bit atau 16 karakter, Oleh karena itu, algoritma kriptografi AES-128 sangat sesuai untuk meng*encrypt text* pada *file* yang terdiri dari baris demi baris *text* dengan panjang lebih dari 16 karakter. [8]Dengan demikian, penggunaan AES-128 dalam sistem keamanan akan membantu menjaga kerahasiaan dan integritas data penjualan Toko Kayu Jati Nadia dari akses yang tidak sah.

Penelitian ini telah menerapkan algoritma kriptografi AES-128 secara langsung setelah melakukan penelitian menggunakan algoritma RSA untuk memastikan keamanan *file*. Hasil dari pengujian dengan kompresi *Huffman* menunjukkan bahwa algoritma AES memiliki kecepatan yang lebih baik dibandingkan dengan algoritma RSA. Algoritma AES menunjukkan kinerja waktu enkripsi dan dekripsi yang lebih efisien dibandingkan dengan RSA, dan menghasilkan ukuran karakter terenkripsi yang lebih kecil.

2. METODE PENELITIAN

2.1 Pengumpulan Data

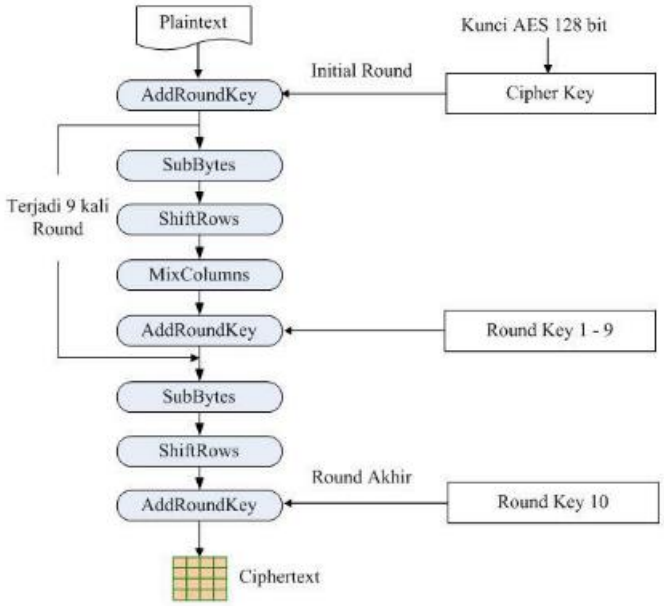
Pada fase ini, data dan informasi yang relevan dengan permasalahan yang ada dikumpulkan. Proses pengumpulan data dan informasi ini melibatkan wawancara serta observasi. Wawancara Tahap-tahap tersebut

dilaksanakan atau dijalankan dengan mengajukan pertanyaan kepada pihak tempat riset yang memiliki keterkaitan dengan pengamanan dokumen yang dilakukan oleh pemilik toko. Tujuannya adalah untuk memperoleh informasi tentang sistem pengamanan dokumen yang digunakan. Selanjutnya, observasi dilakukan dengan mengamati langsung dari prosedur sistem keamanan dokumen yang sedang diimplementasikan di tempat riset tersebut.[9]

2.2 Penerapan Metode

Dalam fase ini dijelaskan mengenai proses enkripsi dan dekripsi menggunakan algoritma AES-128. Berikut adalah langkah-langkah untuk melakukan enkripsi pada Algoritma AES-128: [10]

a. Tahap *AddRoundKey* melakukan operasi XOR antara *state* awal (*plaintext*) dengan *cipher key*. Tahap ini juga sering disebut *initial round*.
b. Selama putaran sebanyak Nr-1 kali, dilakukan proses berikut:
    1. *SubBytes*: penggantian *byte* dengan menggunakan tabel substitusi (S-box).
    2. *ShiftRows*: Melakukan penggeseran pada baris-baris dalam array state dengan cara melingkup.
    3. *MixColumns*: Melakukan proses pengacakan data pada setiap kolom dalam *array state*.
    4. *AddRoundKey* : Melakukan operasi XOR antara *state* saat ini dengan *round key*.
c. Tahap *Final Round* Proses untuk putaran terakhir melibatkan langkah-langkah berikut:
    1. *SubBytes*.
    2. *ShiftRows*.
    3. *AddRoundKey*.



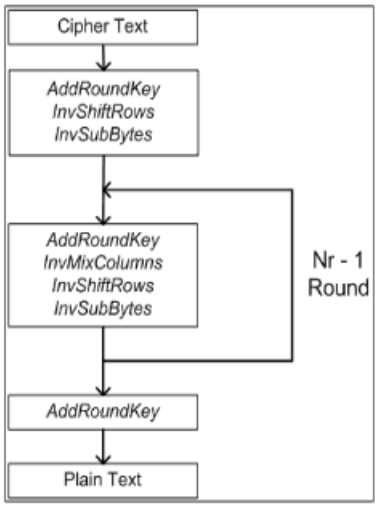
Gambar 1. Proses Enkripsi AES-128

Di bawah ini adalah langkah-langkah untuk melakukan dekripsi pada Algoritma AES-128.[11]

a. Pada tahap *AddRoundKey*, dilakukan operasi XOR pada *state* awal (*plaintext*) dengan *chiperkey*. Proses ini juga sering disebut sebagai tahap awal (*initial round*).
b. Putaran dilakukan sebanyak Nr-1 kali. Pada setiap putaran, proses yang dijalankan adalah sebagai berikut:
    1. *InverseShiftRows* : proses pergeseran baris demi baris pada *array state* dengan terbalik (*inverse*) dari proses *ShiftRows*. Pada tahap *InverseShiftRows*, setiap baris dari *array state* digeser ke arah sebaliknya (dari kanan ke kiri) sebagai langkah pembalikan dari proses *ShiftRows* sebelumnya.
    2. *InverseSubBytes* : proses substitusi *byte* dengan menggunakan tabel *invers* substitusi (*inverse S-box*). Pada tahap *InverseSubBytes*, setiap *byte* pada *array state* digantikan oleh *byte* yang sesuai dari tabel *invers* substitusi (*inverse S-box*) untuk melakukan pembalikan dari proses *SubBytes* sebelumnya.

3. *AddRoundKey* : tahap yang melakukan operasi XOR pada *state* saat ini dengan *round key*. Pada tahap ini, setiap *byte* dari *state* di-XOR dengan *byte* yang sesuai dari *round key* yang dihasilkan pada langkah sebelumnya.
4. *InverseMixColumns* : tahap yang melakukan pembalikan (*inverse*) dari operasi *MixColumns*. Pada tahap *InverseMixColumns*, dilakukan transformasi pada setiap kolom dari *state* menggunakan matriks *invers* khusus untuk mengembalikan *state* ke bentuk sebelumnya setelah dilakukan operasi *MixColumns* sebelumnya.

c. *Final Round* : merupakan tahap terakhir pada proses enkripsi atau dekripsi pada algoritma AES-128 : [12]
   1. *InverseShiftRows*
   2. *InverseSubBytes*
   3. *AddRoundKey*



Gambar 2. Proses Dekripsi AES-128

2.3 Perancangan Perangkat Lunak

Didalam tahap perancangan ini melibatkan perancangan yang didasarkan dari hasil analisis sistem, Khususnya untuk perancangan pada modul *encrypt* dan *decrypt*, disertakan desain antarmuka merupakan bagian dari tahap ini. Pengembangan perangkat lunak akan dilakukan menggunakan pendekatan konvensional, yakni metode *waterfall*. Dalam model ini, setiap fase harus diselesaikan sepenuhnya sebelum memasuki fase selanjutnya, dan setiap hasil dari setiap fase harus didokumentasikan secara komprehensif.

2.4 Implementasi

Selama proses ini, sistem diimplementasikan dengan mengembangkan aplikasi yang sesuai dengan kebutuhan sistem berdasarkan desain sebelumnya yang telah diimplementasikan. Pada tahap implementasi ini, dilakukan pengembangan aplikasi sesuai dengan desain yang telah dibuat sebelumnya melibatkan proses mengubah modul-modul yang sudah direncanakan untuk tahap desain menjadi kode bahasa pemrograman tertentu. Dalam situasi ini, aplikasi yang akan digunakan adalah Aplikasi kriptografi yang mengadopsi algoritme AES-128.

2.5 Pengujian Sistem

Pada tahap pengujian sistem, diberlakukan serangkaian uji coba terhadap sistem yang sudah dikembangkan. Tujuan dari tahap ini adalah memastikan apakah pada sistem yang telah dibangun sesuai dengan dari hasil analisis dan apabila pada rancangan untuk aplikasi ini berfungsi sebagaimana yang diharapkan. Dalam tahap ini, digunakan metode pengujian *blackbox testing* yang bertujuan untuk mengevaluasi aplikasi secara keseluruhan dan menemukan potensi *bug* serta melakukan pengujian fungsional. *Blackbox testing* memungkinkan evaluasi terhadap bagaimana aplikasi merespon input dan menghasilkan *output* yang sesuai dengan yang diinginkan.

2.6 Kesimpulan

Pada proses tahap kesimpulan, dilakukan kesimpulan akhir yang terkait efektivitas penggunaan pengamanan metode kriptografi *Advanced Encryption Standard* (AES) untuk menjaga keamanan *file*. Dengan merujuk pada hasil pengujian sistem yang sudah dilaksanakan, Dengan merujuk pada hasil pengujian yang sudah dilaksanakan, disarankan kembali untuk melakukan perbaikan dan pengembangan yang lebih lanjut untuk sistem yang sudah ada agar disaat melakukan penerapan pada metode *Advanced Encryption Standard* (AES) dapat menghasilkan tingkat keamanan yang optimal pada *file* tersebut. Sehingga, direkomendasikan untuk melakukan upaya perbaikan serta pengembangan lebih lanjut lagi terhadap sistem yang telah diimplementasikan.

2.7 Spesifikasi *Database*

Pada aplikasi ini, didapati basis data yang menggunakan struktur-struktur tabel berikut untuk mendukung pembuatan aplikasi. Tabel 1 spesifikasi dari *database user* dan Tabel 2 merupakan spesifikasi dari *database file*.

a. Nama *Database* : kriptografi2
   Nama Tabel : *User*
   Media : *Hardisk*
   Primary Key : id_*user*

Tabel 1. Spesifikasi pada Tabel *User*

Nama *Field*	*Type*	*Length*	Keterangan
Id_*user*	Int	5	Kode pengguna
Nama	Varchar	100	Nama Pengguna
Email	Varchar	100	*Email* pengguna
Password	Varchar	255	*Password*
Role	Int	1	*Role* pengguna

b. Nama *Database* : kriptografi2
   Nama Tabel : *File*
   Media : *Hardisk*
   Primary Key : id_*file*

Tabel 2. Spesifikasi pada Tabel *File*

Nama *Field*	*Type*	*Length*	Keterangan
Id_*file*	Int	11	Kode *file*
Upload_by	Int	15	Nama Pengguna yang *upload*
File_name_source	Varchar	255	Nama *file* awal
File_name_finish	Varchar	255	Nama *file* akhir
File_url	Timestamp	255	Nama url
File_size	Float		Ukuran *file*
Password	Varchar	16	*Password* / Kunci AES 128
Tgl_*upload*	DateTime	6	Tanggal *Upload*

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

Pada lingkungan percobaan, akan disediakan spesifikasi yang dibutuhkan untuk mengembangkan aplikasi untuk pengamanan dokumen yang menerapkan Algoritme *Advanced Encryption Standard* (AES-128) di Toko Kayu Jati Nadia agar aplikasi tersebut dapat berfungsi dengan baik. Spesifikasi yang akan digunakan untuk mengembangkan aplikasi ini harus sesuai dengan kebutuhan dan mendukung fungsionalitas yang diinginkan.

Untuk perangkat keras yang akan digunakan dalam pembuatan aplikasi ini, akan digunakan prosesor *Intel Core i3-8145U* dengan kecepatan *2.1 GHz*, *RAM* atau memori sebesar 4GB, dan penyimpanan SSD sebesar 512GB. Spesifikasi ini dipilih agar aplikasi dapat berjalan dengan kinerja yang memadai dan responsif.

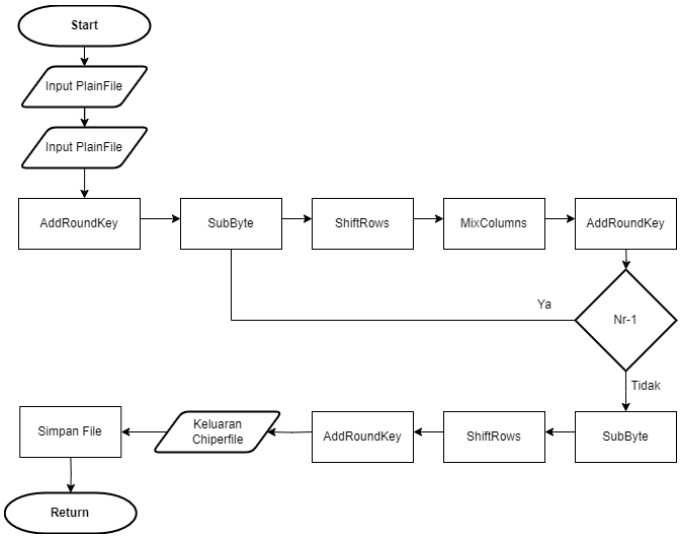
Sementara itu, untuk perangkat lunak yang akan digunakan dalam pembuatan aplikasi pengamanan dokumen, akan digunakan Sistem Operasi *Windows 11* sebagai *platform* utama. Selain itu, perangkat lunak lain yang akan dipakai adalah *MySQL* sebagai sistem manajemen basis data, *Visual Studio Code* sebagai *editor* kode, XAMPP sebagai *platform* untuk mengembangkan dan menguji aplikasi berbasis web, dan *Google Chrome* sebagai *browser* untuk mengakses dan menguji aplikasi.

3.2 *Flowchart*

Flowchart atau diagram alur adalah Gambaran visual tersebut mengilustrasikan langkah demi langkah dan keputusan yang harus diambil dalam menjalankan proses didalam sebuah program secara grafis. Pada setiap langkahnya dalam proses tersebut direpresentasikan melalui banyaknya simbol khusus dan dihubungkan langsung dengan garis atau anak panah yang berguna untuk mengilustrasikan hubungan antar langkah-langkah proses tersebut secara *visual*. *Flowchart* membantu untuk memvisualisasikan jalur eksekusi dan logika dari suatu program secara jelas dan mudah dipahami.

3.3 *Flowchart* Proses Enkripsi

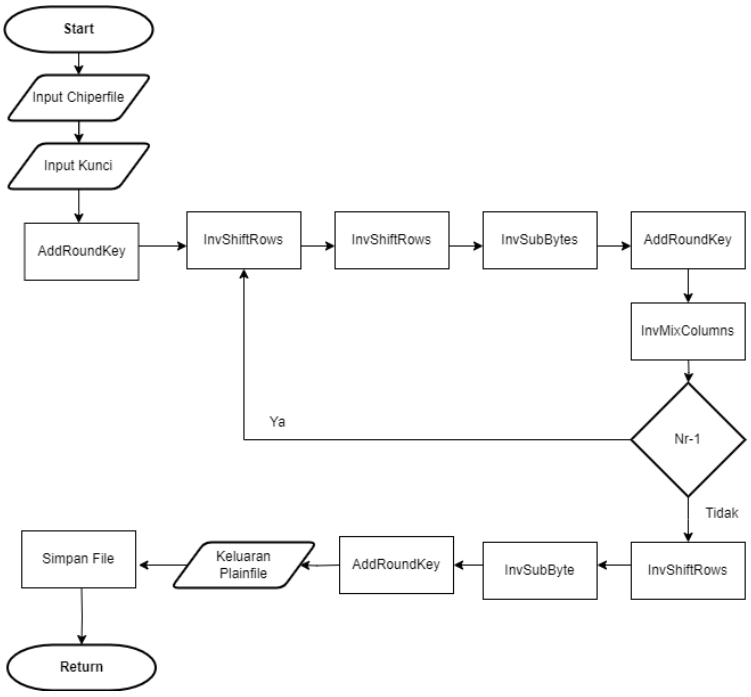
Gambar 3 merupakan sebuah *flowchart* yang menggambarkan alur proses enkripsi pada Algoritme *Advanced Encryption Standard* (AES). *Flowchart* ini menjelaskan langkah-langkah yang terjadi pada algoritme AES-128 untuk mengenkripsi *Plaintext*. *Flowchart* tersebut terdapat pada Gambar 3, dan ia memberikan gambaran tentang proses enkripsi yang dilakukan oleh algoritme AES-128 secara *visual*.



Gambar 3. *Flowchart* Proses Enkripsi

3.4 *Flowchart* Proses Dekripsi

Gambar 4 adalah *flowchart* yang menggambarkan alur proses dekripsi pada Algoritma *Advanced Encryption Standard* (AES). *Flowchart* tersebut menjelaskan langkah-langkah yang terjadi pada algoritma AES-128 untuk men*decrypt ciphertext*, sehingga mengembalikan ke bentuk *Plaintext* aslinya.

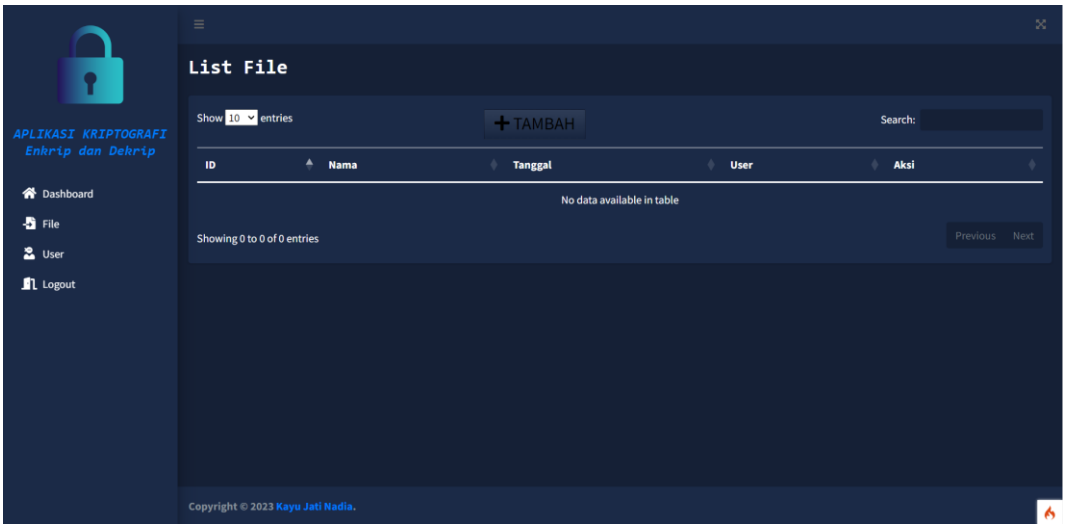


Gambar 4. *Flowchart* Proses Dekripsi

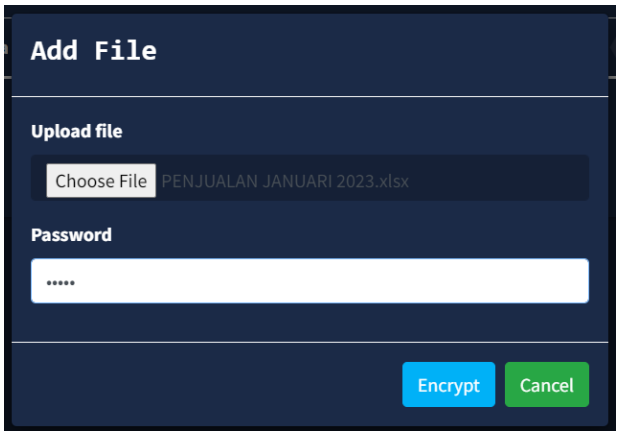
3.5 Tampilan Layar Halaman File

Pada bagian menu *file*, terdapat sebuah tabel yang berfungsi untuk melakukan proses *encrypt* dan *decrypt file*. Pengguna juga memiliki opsi untuk memilih jumlah *file* yang terenkripsi yang ingin mereka tampilkan. Apabila pengguna berkeinginan untuk *encrypt file*, untuk langkah pertama yang harus diambil adalah mengklik *button* "Tambah". Setelah itu, mereka dapat memilih *file* mana yang ingin di*encrypt* dan meng*input* password sesuai dengan preferensi mereka. Ketika proses enkripsi selesai, pengguna dapat menggunakan *submenu* yang sama untuk melakukan dekripsi. Dalam proses dekripsi, Pengguna hanya bisa memasukkan password yang sama dengan yang digunakan saat melakukan proses enkripsi.

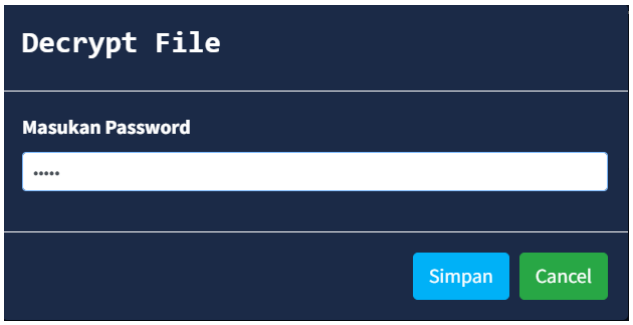
Berikut ini adalah gambaran dari tampilan pada layar submenu *File* pada Gambar 5, tampilan pada layar proses enkripsi pada Gambar 6, serta tampilan pada layar proses dekripsi pada Gambar 7.



Gambar 5. Tampilan pada Layar Halaman *File*



Gambar 6. Tampilan pada Layar Enkripsi *Add File*



Gambar 7. Tampilan pada Layar Dekripsi

3.6 Pengujian

Pengujian aplikasi ini adalah sebuah penelitian yang bertujuan untuk mendapatkan informasi mengenai performa Sistem aplikasi keamanan *file* di Toko Kayu Jati Nadia diuji melalui dua tahap, Dalam pengujian tersebut, terdapat dua tahap yang melibatkan pengujian proses enkripsi *file* dan pengujian proses dekripsi *file*.

3.6.1 Hasil Pengujian

Berikut adalah hasil dari pengujian yang telah dilakukan terhadap jenis *file* yang ada pada Toko Kayu Jati Nadia dengan ekstensi xlsx, Hasil pengujian tersebut diberitahukan dalam Tabel 3 serta Tabel 4 yang merupakan hasil dari proses *encrypt* serta *decrypt*.

Tabel 3. Tabel Hasil Pengujian Enkripsi

Nama Awal File	Ukuran File Asli (Byte)	Nama File Setelah Di Enkripsi	Ukuran File Setelah Enkripsi (Byte)	Durasi Enkripsi (Milidetik)
PENJUALAN JUNI 2022.xlsx	18.528	61784-penjualan-juni-2022.rda	18.528	560
PENJUALAN JULI 2022.xlsx	19.776	36469-penjualan-juli-2022.rda	19.776	670
PENJUALAN AGUSTUS 2022	17.920	83239-penjualan--agustus-2022.rda	17.920	520
PENJUALAN SEPT 2022	18.992	16950-penjualan-sept-2022.rda	18.992	570
PENJUALAN OKTOBER 2022	18.080	55799-penjualan--oktober-2022.rda	18.080	660
PENJUALAN NOP 2022	18.416	76482-penjualan--nop-2022.rda	18.416	580
PENJUALAN DESEMBER 2022	17.872	25479-penjualan-desember-2022.rda	17.872	570

PENJUALAN JANUARI 2023	18.224	21215-penjualan-januari-2023.rda	18.224	580
PENJUALAN FEBRUARI 2023	18.816	97171-penjualan-februari-2023.rda	18.816	560
PENJUALAN MARET 2023	18.896	43471-penjualan-maret-2023.rda	18.896	630
PENJUALAN APRIL 2023	18.224	74834-penjualan-april-2023.rda	18.224	530
PENJUALAN MEI 2023	17.600	93501-penjualan-mei-2023.rda	17.600	570
JUMLAH RATA-RATA	18.445		18.445	583

Tabel 4. Tabel Hasil Pengujian Dekripsi

Nama File Enkripsi	Ukuran File Setelah Di Enkripsi (Byte)	Nama File Hasil Dekripsi	Ukuran File Setelah Di Dekripsi (Byte)	Durasi Dekripsi (MiliDetik)
61784-penjualan-juni-2022.rda	18.528	PENJUALAN JUNI 2022.xlsx	18.528	710
36469-penjualan-juli-2022.rda	19.776	PENJUALAN JULI 2022.xlsx	19.776	510
83239-penjualan--agustus-2022.rda	17.920	PENJUALAN AGUSTUS 2022	17.920	490
16950-penjualan-sept-2022.rda	18.992	PENJUALAN SEPT 2022	18.992	480
55799-penjualan--oktober-2022.rda	18.080	PENJUALAN OKTOBER 2022	18.080	490
76482-penjualan--nop-2022.rda	18.416	PENJUALAN NOP 2022	18.416	480
25479-penjualan-desember-2022.rda	17.872	PENJUALAN DESEMBER 2022	17.872	500
21215-penjualan-januari-2023.rda	18.224	PENJUALAN JANUARI 2023	18.224	480
97171-penjualan-februari-2023.rda	18.816	PENJUALAN FEBRUARI 2023	18.816	490
43471-penjualan-maret-2023.rda	18.896	PENJUALAN MARET 2023	18.896	470
74834-penjualan-april-2023.rda	18.224	PENJUALAN APRIL 2023	18.224	480
93501-penjualan-mei-2023.rda	17.600	PENJUALAN MEI 2023	17.600	460
JUMLAH RATA-RATA	18.445		18.445	503

Maka dapat disimpulkan hasil akhir dari proses pengujian *file* rata-rata besar ukuran hasil enkripsi *file* adalah 18.445 *bytes*, kemudian rata-rata waktu pemrosesan enkripsi adalah 583 milidetik. Lalu ada hasil akhir dari proses rata-rata ukuran hasil besar *file* dekripsi adalah 18.445 *bytes* dan rata-rata waktu pemrosesan dekripsi adalah 503 milidetik.

4. KESIMPULAN

Berdasarkan hasil analisis yang sudah dilakukan kepada permasalahan dan hasil dari pengujian yang telah dilakukan pada aplikasi untuk pengamanan dokumen yang menerapkan algoritma kriptografi dengan metode *Advanced Encryption Standard* (AES-128), dapat disimpulkan bahwa aplikasi ini efektif dalam mengamankan dokumen Toko Kayu Jati Nadia dan mencegah kebocoran data. Hasil akhir dari proses pengujian *file* rata-rata besar ukuran hasil enkripsi *file* adalah 18.445 *bytes*, kemudian rata-rata waktu pemrosesan enkripsi adalah 583 milidetik. Lalu ada hasil akhir dari proses rata-rata ukuran hasil besar *file* dekripsi adalah 18.445 *bytes* dan rata-rata waktu pemrosesan dekripsi adalah 503 milidetik.

DAFTAR PUSTAKA

[1] 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.

[2] L. Laurentinus, H. A. Pradana, D. Y. Sylfania, and F. P. Juniawan, "Performance comparison of RSA and AES to SMS messages compression using Huffman algorithm," *J. Teknol. dan Sist. Komput.*, vol. 8, no. 3, pp. 171–177, 2020, doi: 10.14710/jtsiskom.2020.13468.

[3] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

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

[5] U. E. Amrulloh A, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.

[6] Donzilio Antonio Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[7] Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[8] 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.

[9] 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.

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

[11] S. D. Nurcahya, "Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 5, no. 4, pp. 694–697, 2022, doi: 10.32672/jnkti.v5i4.4690.

[12] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 6, no. 1, pp. 1–10, 2019, doi: 10.33330/jurteksi.v6i1.395.