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

# PENERAPAN KRIPTOGRAFI MENGGUNAKAN ALGORITME *ADVANCED ENCRYPTION STANDARD(AES-128)* UNTUK MENGAMANKAN DATA PENGIRIMAN CUSTOMER AGEN JNE ANDARA

**Tomi Muammar Mudo[1], Ferdiansyah[2*], Ika Susanti[3]**
[1]Teknik Informatika, Fakultas Teknologi Indormasi, Universitas Budi Luhur, Jakarta, Indonesia
Email: [1]1911511747@student.budiluhur.ac.id [2*]Ferdiansyah@budiluhur.ac.id, [3]ika.susanti@budiluhur.ac.id
(* : corresponding author)

**Abstrak-**Perkembangan teknologi saat ini sangat membawa dampak yang besar pada era digital ,Penelitian ini bertujuan untuk mengimplementasikan kriptografi menggunakan algoritme *Advanced Encryption Standard* (AES-128) guna meningkatkan keamanan data pengiriman customer pada agen JNE Andara. Data pengiriman customer di JNE Andara mengandung informasi sensitif seperti alamat, nomor telepon, dan detail pesanan, yang perlu dijaga kerahasiaannya agar tidak jatuh ke tangan yang salah. Oleh karena itu, diperlukan sistem keamanan yang dapat mengenkripsi data tersebut sehingga hanya dapat diakses oleh pihak yang berwenang. Metode yang digunakan dalam penelitian ini adalah algoritme AES-128 pada sistem pengiriman data customer di agen *JNE Andara*. Algoritme AES-128 dipilih karena telah diakui secara internasional sebagai standar enkripsi yang aman dan efisien. Penelitian ini melibatkan pengembangan perangkat lunak yang memanfaatkan algoritme AES-128 untuk mengenkripsi data pengiriman customer sebelum dikirim melalui jaringan. Hasil dari penelitian ini menunjukkan bahwa implementasi kriptografi menggunakan algoritme AES-128 dapat efektif meningkatkan keamanan data pengiriman customer pada agen JNE Andara. Dengan menerapkan enkripsi AES-128,data pengiriman customer dapat dienkripsi sebelum dikirim melalui jaringan, sehingga hanya pihak yang memiliki kunci enkripsi yang benar dapat membaca dan memproses data tersebut. Ini memberikan perlindungan tambahan terhadap ancaman pengintaian dan peretasan data yang mungkin terjadi selama proses pengiriman. Penelitian ini memberikan rekomendasi kepada agen JNE Andara untuk menerapkan kriptografi menggunakan algoritme AES-128 sebagai langkah penting dalam meningkatkan keamanan data pengiriman customer. dapat disimpulkan bahwa aplikasi ini mampu untuk mengamankan dan menjaga isi file data pengiriman penting JNE Andara. Kontribusi penelitian ini adalah untuk mengatasi kebocoran atau pencurian data berupa file data pengiriman pada Agen JNE Andara. Hasil dari penelitian ini menunjukkan bahwa file berhasil dienkripsi dan memastikan keamanan file tersebut terjaga.

**Kata Kunci:** *Advanced Encryption standard* (AES-128), Kriptografi, JNE Andara ,data pengiriman customer

# *IMPLEMENTATION OF CRYPTOGRAPHY USING ADVANCED ENCRYPTION STANDARD(AES-128) ALGORITHM TO SECURE DATA DELIVERY OF CUSTOMER AGENT JNE ANDARA*

**Abstract-** *Current technological developments have had a major impact on the digital era. This study aims to implement cryptography using the Advanced Encryption Standard (AES-128) algorithm to increase the security of customer data delivery at JNE Andara agents. Customer shipping data at JNE Andara contains sensitive information such as addresses, telephone numbers, and order details, which need to be kept confidential so they don't fall into the wrong hands. Therefore, a security system is needed that can encrypt the data so that it can only be accessed by authorized parties. The method used in this study is the AES-128 algorithm on the customer data delivery system at the JNE Andara agent. The AES-128 algorithm was chosen because it has been internationally recognized as a secure and efficient encryption standard. This research involves the development of software that utilizes the AES-128 algorithm to encrypt customer delivery data before it is sent over the network. The results of this study indicate that the implementation of cryptography using the AES-128 algorithm can effectively improve the security of customer delivery data at JNE Andara agents. By implementing AES-128 encryption, customer delivery data can be encrypted before being sent over the network, so that only those who have the correct encryption key can read and process the data. This provides additional protection against data snooping and hacking threats that may occur during the transmission process. This study provides recommendations to JNE Andara agents to apply cryptography using the AES-128 algorithm as an important step in increasing the security of customer delivery data. it can be concluded that this application is able to secure and maintain the contents of JNE Andara's important delivery data files. The contribution of this research is to overcome data leaks or theft in the form of sending data files to JNE Andara Agents. The results of this study indicate that the file was successfully encrypted and ensured that the security of the file is maintained.*

***Keywords****: Advanced Encryption standard (AES-128), Cryptography, JNE Andara, customer delivery data*

# 1. PENDAHULUAN

Perkembangan teknologi di masa sekarang terjadi dengan cepat, hal ini terbukti dengan semakin meningkatnya peranan teknologi dalam berbagai bidang kehidupan. Kemajuan teknologi telah membuat proses komunikasi menjadi lebih cepat dan efisien. Hal ini tidak terlepas dari terjadinya berbagai tindakan penyadapan dan pemantauan oleh pihak-pihak yang sebenarnya tidak berkepentingan ,sehingga informasi yang disampaikan melalui sarana komunikasi menjadi kurang terjaga kerahasiaannya. Agen JNE andara merupakan salah satu jasa kirim yang ada saat ini JNE andara mempunyai banyak data customer yang saat ini masih mengirimkan data pengiriman ke customer secara manual seperti info *e-mail*, no hp dan alamat yang rawan untuk di salahgunakan oleh pihak yang tidak bertanggung jawab Oleh karena itu, diperlukan sistem keamanan yang dapat mengenkripsi data tersebut sehingga hanya dapat diakses oleh pihak yang berwenang.

Berdasarkan latar belakang diatas, maka dibutuhkan suatu cara untuk dapat mengamankan data pengiriman customer, teknik pengamanan yang digunakan adalah dengan kriptografi, kriptografi dapat diartikan menjadi tulisan rahasia. Kriptografi adalah ilmu tentang teknik enkripsi yang dimana data diacak dengan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh orang yang tidak mempunyai kunci dekripsi[1]. Dalam bidang kriptografi terdapat dua konsep yang sangat penting yaitu enkripsi dan deskripsi. Proses pengiriman pesan akan melalui proses enkripsi untuk mengubah teks asli (*plaintext*) menjadi teks sandi *(ciphertext*). Dengan proses enkripsi suatu informasi akan menjadi lebih sulit untuk diketahui oleh orang yang tidak berhak [2]. Untuk dapat menjalankan dengan baik pada proses kriptografi haruslah terdapat empat elemen utama didalamnya, yang paling berkait satu sama lain yaitu *plaintext,chipertext,cryptography key* dan *encryption decryption* algoritm [3]. Kriptografi memiliki aspek aspek dan tujuan dengan memberikan keamanan yaitu *Confidentially*(kerahasiaan*), Data Integrity*/, *Authentication*/(Autentifikasi) dan *Non-repudiation*/(penyangkalan)[4]

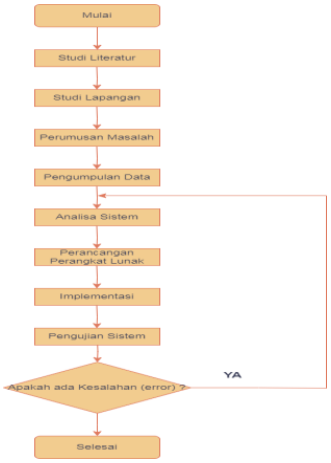
Berdasarkan Pada Penelitian lain yang berjudul implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa [2]Penelitian ini mengimplementasikan kriptografi menggunakan algoritme AES-128 maka diperoleh hasil bahwa isi file soal ujian asli (plaintext) yang dienkripsi menggunakan AES-128 dapat terenkripsi dengan baik, hal ini terbukti dari isi file soal ujian yang hasilkan tidak dapat dimengerti oleh pengguna, kemudian setelah isi file soalujian tersebut dideskripsi, maka akan kembali seperti data awal yang diinputkan. Waktu darihasil uji enkripsi dan dekripsidarisembilan file soal uji menu njukkanbahwa rata-rata wak tu enkripsi adalah 1,3108 detik dan waktu dekripsi rata-rata 1,5532 detik, denganukuran file kurangdari 3MB relatif cepat yaitu kurang dari 4 detik. AES sendiri merupakan algoritme perkembangan dari algoritme DES, dimana jika keduanya dibandingkan AES sendiri memerlukan waktu yang jauh lebih singkat ketika melakukan enkripsi dan dekripsi [6]. Dan algoritme AES dapat mengubah informasi menjadi *ciphertext* melalui enkripsi dan mengembalikan lagi *ciphertext* menjadi *plaintext* melalui proses dekripsi. AES ini menggunakan kunci kriptografi dengan panjang key 128, 192, atau 256 bit untuk mengenkripsi dan mendekripsi data pada reel 128-bit [7]. Proses enkripsi algoritme AES terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*[8]. Sedangkan pada proses dekripsi mengunakan *invers* semua transformasi dasar pada algoritma AES kecuali *addroundkey* dengan urutan transformasi *invshiftrows*, *invsubbytes*, *addroundkey*,dan *invmixcolumns*.[9]. Dengan demikian dapat disimpulkan bawah algoritme AES dapat mengamankan semua jenis *file* dan juga algoritme AES (*Advanced Encryption Standard*) dipilih karena mempunyai keamanan yang sangat tinggi dan kebal dari berbagai macam serangan, dan juga karena kesederhanaan desain, kekompakan kode dan kecepatan ketika men-enkripsi dan deskripsi data atau file [10]

Pada Penelitian lain [3] yang berjudul Implementasi Algoritma Kriptografi AES Advanced Encryption Standard 128 Bit Untuk Pengamanan Dokumen Shipping tujuan peneliti adalah menggunakan teknik deskripsi-enkripsi dengan algoritma AES 128-bit menjadi sistem karena memiliki tingkat ketahanan terhadap segala jenis serangan untuk menghindari kehilangan dan pencurian serta mengurangi resiko kerusakan data/file.

Oleh karena itu Tujuan dari penelitian menggunakan metode AES-128 ini adalah agar data yang tersimpan dapat terjaga dengan baik dan perusahaan tempat penelitian ini dilakukan dapat terbantu dengan baik dalam pengelolaan, pengiriman dan keamanan file dokumen tersebut agar tetap baik. Kontribusi penelitian ini adalah untuk mengatasi kebocoran atau pencurian data berupa file data pengiriman pada Agen JNE Andara. Hasil dari penelitian ini menunjukkan bahwa file berhasil dienkripsi dan memastikan keamanan file tersebut terjaga.

# 2. METODE PENELITIAN

## 2.1 Penerapan Metode



Pada **gambar 1** Penerapan metode adalah serangkaian langkah sistematis yang digunakan oleh peneliti untuk merancang, mengumpulkan, menganalisis, dan menyajikan data dalam rangka menjawab pertanyaan penelitian atau mencapai tujuan penelitian tertentu. Penerapan metode membantu memastikan bahwa penelitian dilakukan secara terstruktur, obyektif, dan dapat diandalkan sehingga menghasilkan hasil yang baik dan dapat di pertanggungjawabkan.

Berikut tahapan penerapan metode yang ditulis oleh penulis :

a. Studi Literatur

Pada tahap ini dilakukan studi dengan mempelajari berbagai macam buku jurnal dan karya tulis ilmiah yang berkaitan dengan masalah yang akan dibahas yaitu pengamanan data khususnya dengan menggunakan metode kriptografi *Advanced Encryption Standard* (AES)

b. Studi Lapangan

Dalam tahap ini kita melakukan studi kasus tehadap *file* yang berada di JNE Andara sehingga permasalahan yang ada dapat di indetifikasi dan kemudian *file* itu dapat dirumuskan saat menyelesaikan permasalahan.

c. Perumusan Masalah

Pada tahap ini ditentukan masalah yang akan di selesaikan dalam penelitian ini yaitu pengamanan data pengiriman customer,data invoice customer pada agen JNE AndaraDengan menggunakan metode implementasi Algoritma Advanced Enkryption Standard (AES) yang akan dilakukan di dalam program dan akan di uji enkripsi dan deskripsi nya agar data yang di kirim tetap aman Kembali.

d. Pengumpulan Data

1. Observasi
   Penelitian ini menggunakan metode pengumpulan data dengan melakukan observasi langsung terhadap kejadian di lapangan. Fokus penelitian adalah meninjau secara langsung kegiatan proses pengiriman data di Agen JNE Andara. Kegiatan observasi meliputi pengambilan data pengirim seperti nama, alamat, nomor resi, dan nomor telepon.
2. Wawancara
   Wawancara adalah suatu cara pengumpulan data dengan melakukan pertemuan tatap muka dan berbicara dengan pemilik Agen JNE Andara serta admin yang bertanggung jawab dalam menginput data pengiriman. Tujuan dari proses ini adalah untuk mendapatkan data dan informasi terkait pengelolaan data pengiriman yang sedang berlangsung saat ini.
3. Dokumentasi
   Dalam proses dokumentasi, penulis meminta kepada Admin JNE Andara untuk memberikan data-data yang diperlukan dan yang sudah tersedia di JNE Andara. Data ini akan digunakan sebagai masukan dalam pembuatan sistem aplikasi.

e. Analisa sistem

Pada tahap ini adalah tahap mengidetifikasi atau menganalisis masalah sistem yang disesuaikan dengan batasan yang ada.dalam mengidentifikasi masalah tersebut,analisis yang diperlukan untuk memecahkan masalah penelitian ini.

f. Perancangan Perangkat Lunak

Pada tahap ini perencanaan didasarkan pada hasil analisis sistem yaitu dari modul enkripsi dan dekripsi dan modul pendukung terkait lainnya dirancang, yang dapat segera diintegrasikan ke dalam program, dan antarmuka pengguna dirancang, yang membutuhkan langkah kerja untuk diselesaikan sebelum melanjutkan ke langkah berikutnya, dan hasil dari masing-masing langkah harus. akurat untuk dicatat.

g. Implementasi

Pada proses implementasi ini dilakukan pembuatan yang telah dirancang dalam tahap perancangan ke dalam Bahasa pemograman tertentu. Dalam hal ini aplikasi ini digunakan:

a) Aplikasi Perangkat lunak di dalam proses penerapan pengamanan data *file* menggunakan bahasa pemograman php serta DBMS yang digunakan adalah PHPMyAdmin.
b) Menggunakan Perangkat keras dengan *Prosesor* Intel Core i5, RAM 8GB , SSD 512GB

h. Pengujian Sistem

Pada tahap ini ini melibatkan metode pengujian *blackbox testing* dalam melakukan percobaan sistematis, yang tujuannya adalah untuk memastikan bahwa sistem yang digunakan memiliki hasil analisis dan desain, sehingga kesimpulan dapat ditarik apakah sistem akan memberikan hasil yang diinginkan.

## 2.2 Kajian Pustaka

Kajian pustaka adalah proses dalam penelitian di mana peneliti mengumpulkan, mengevaluasi, dan menganalisis literatur yang relevan yang telah ada sebelumnya dalam bidang tertentu. Tujuan dari kajian pustaka adalah untuk memahami penelitian sebelumnya, teori-teori, konsep-konsep, dan perkembangan dalam subjek yang sedang dipelajari. Ini membantu peneliti dalam merumuskan masalah penelitian, mengembangkan kerangka teoritis, dan mengarahkan pendekatan penelitian yang akan diambil.

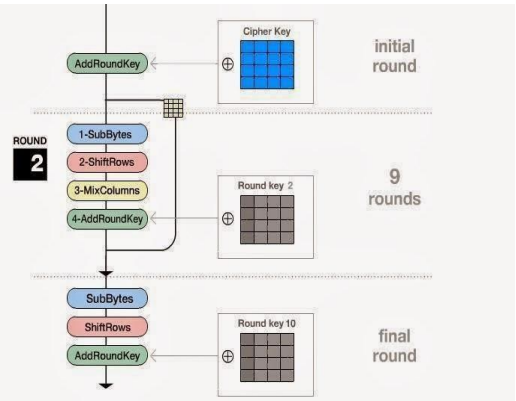
## 2.3 Kriptografi

Kriptografi adalah seni dalam menjaga kerahasiaan pesan. Pesan atau data yang belum diubah dan masih dalam bentuk aslinya disebut sebagai plaintext. Namun, setelah melalui proses penyandian dengan kriptografi, plaintext ini berubah menjadi ciphertext. *ciphertext.*[11]

## 2.4 *Advanced Encryption Standard* (AES-128)

Dalam bagian ini menjelaskan tentang proses enkripsi dan dekripsi algoritma AES-128. Berikut adalah tahapan enkripsi pada Algoritma AES-128[12] :

a. *AddRoundKey :* yaitu proses melakukan XOR terhadap *state* awal (*plaintext*) dan *chiperkey.*
   langkah ini disebut dengan *initial round.*
b. *Round :* yaitu, putaran sebanyak NR – 1 kali. Pada setiap putaran atau ronde memiliki beberapa proses, diantaranya adalah:
   1. *SubBytes :* yaitu, mensubstitusikan *byte* dengan menggunakan table S-box (tabel substitusi).
   2. *ShiftRows :* yaitu, melakukan pergeseran tiap baris array *state* secara *wrapping.*
   3. *Mixcolumn :* yaitu, mengacak data pada tiap kolom array *state.*
   4. *AddRoundKey :* yaitu, melakukan X-OR antara hasil state sekarang dengan kunci hasil proses *expand key.*
c. *Final Round :* yaitu proses untuk putaran atau ronde terakhir:
   1. *SubBytes*
   2. *ShiftRows*
   3. *AddRoundKey*



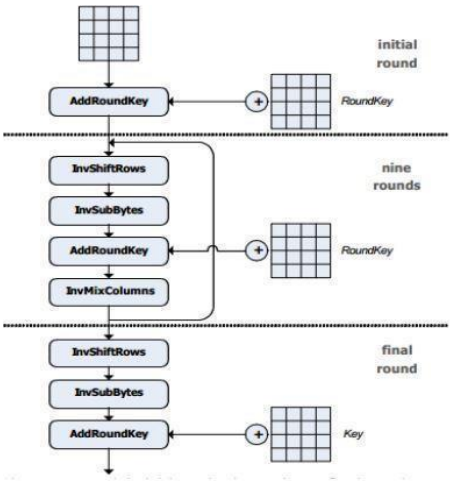

**Gambar 2.** Proses Enkripsi AES-128

Pada **gambar 2** proses enkripsi AES 128 menggambarkan langkah-langkah yang harus diikuti untuk mengenkripsi blok data dengan menggunakan kunci enkripsi 128-bit. Tahap-tahap *SubBytes, ShiftRows, MixColumns, dan AddRoundKey*diulang dalam putaran utama sebanyak 9 kali, diikuti oleh putaran terakhir yang sedikit berbeda.

Berikut adalah tahapan dekripsi pada Algoritme AES-128 [12]:

a. *AddRoundKey* : dengan melakukan XOR antara state awal(*chipertex*) dengan *chiperkey*. Tahap ini disebut juga
   *initial round.*
b. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah :
   1. *InverseShiftRows* : pergeseran baris-baris array *state* secara wrapping kebalikan dari *ShiftRow*s.
   2. *InverseSubBytes* : substitusi *byte* dengan menggunakan tabel invers substitusi ( *invers S*-box).
   3. *AddRoundkey* : melakukan XOR antara state sekarang dengan *round key*.
   4. *InverseMixColumns*: membalikkan operasi MixColumns
c. *Final round* : melakukan proses untuk putaran terakhir :
   1. *InverserShiftRows*

2. *InverseSubBytes*
3. *AddRoundKey*




**Gambar 3.** Proses Dekripsi AES-128

Pada **gambar 3** Proses dekripsi AES menggambarkan langkah-langkah yang harus diikuti untuk mendekripsi blok data yang dienkripsi dengan menggunakan kunci dekripsi yang sesuai. Tahap-tahap *InvShiftRows, InvSubBytes, AddRoundKey, dan InvMixColumns* diulang dalam putaran utama sebanyak 9 kali, diikuti oleh putaran terakhir yang sedikit berbeda.

## *2.5 Blackbox Testing*

*Blackbox Testing* adalah salah satu metode yang sederhana dan praktis karena hanya memerlukan nilai minimum dan maksimum dari data yang diharapkan. Estimasi jumlah data uji dapat dihitung berdasarkan jumlah field data entri yang akan diuji, aturan entri yang harus dipatuhi, serta kasus batas atas dan batas bawah yang relevan. Dengan menggunakan metode ini, kita dapat mengetahui apakah fungsionalitas masih dapat menerima masukan data yang tidak sesuai dengan harapan, sehingga dapat menyebabkan ketidakvalidan data yang disimpan.[13]

## *2.6* Spesifikasi *Database*

a. Tabel user
Nama *Database* : *skripsi_db* Nama table
*:user Primary key* :
username

**Tabel 1.** Spesifikasi Database Tabel *User*

| Nama | Type data | Ukuran | Keterangan |
|---|---|---|---|
| username | varchar | 15 | *Username* |
| Password | varchar | 10 | *Password* |
| fullname | varchar | 50 | Nama user |
| Job_title | varchar | 50 | Jabatan |
| Join_date | timestamp | - | Tanggal bergabung |
| Last activity | timestamp | - | Aktifitas terakhir |
| status | enum | ‘1’,’2’ | Admin dan user |

Pada **tabel 1** Spesifikasi tabel user merupakan panduan yang mendefinisikan struktur dan atribut yang ada dalam tabel yang menyimpan informasi tentang pengguna dalam sebuah database. Spesifikasi ini memberikan panduan tentang bagaimana tabel tersebut harus dirancang, termasuk nama kolom, tipe data, batasan unik, dan properti lainnya.

b. Tabel file
Nama Database : *skripsi_db* Nama table
: *file Primary key* :
id_file

**Tabel 2.** Spesifikasi Database Tabel *file*

| Nama | Type data | Ukuran | Keterangan |
|---|---|---|---|
| id_file | int | 11 | Id *file* |
| username | varchar | 15 | *Username* |
| file_name_source | varchar | 255 | Nama *file* asli |
| file_name_finish | varchar | 255 | Nama hasil *file* |
| file_url | varchar | 255 | Url *file* |
| file_size | float | - | Ukuran *file* |
| password | varchar | 16 | *Password* |
| tgl_upload | timestamp | - | Tanggal upload |
| status | enum | (‘1’.’2’) | Enkripsi dan Dekripsi |
| keterangan | varchar | 255 | Keterangan |
| durasi_enkripsi | varchar | - | Waktu enkripsi |

Pada **tabel 2** Spesifikasi tabel *file* adalah panduan yang mendefinisikan struktur dan atribut yang ada dalam tabel yang digunakan untuk menyimpan informasi terkait berkas atau dokumen dalam sebuah database. Spesifikasi ini memberikan arahan tentang bagaimana tabel tersebut seharusnya dirancang, termasuk kolom-kolom yang diperlukan, tipe data yang digunakan, serta batasan dan properti lainnya.

# 3. HASIL DAN PEMBAHASAN

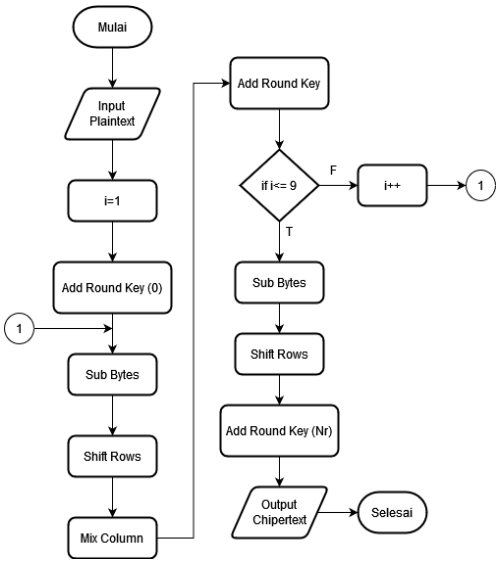
## 3.1 Lingkungan Percobaan

Pada lingkungan percobaan akan diberikan spesifikasi yang diperlukan untuk membuat aplikasi pengamanan file dengan algoritme *Advanced Encryption Standard* (AES 128) pada agen JNE Andara agar bisa digunakan dengan semestinya dan spesifikasi yang akan dipakai untuk membangun aplikasi ini juga harus mendukung. Berikut spesifikiasi yang akan dibuat pada perangkat keras yang dipakai dalam pembuatan alat bantu aplikasi pengamanan file adalah menggunakan *processor* Core i5, RAM 8GB, SSD 512GB. dan perangkat lunak yang digunakan dalam pembuatan aplikasi pengamanan file adalah *Microsoft Windows* 11, MySQL, *Visual Studio Code*, XAMPP dan *Google Chrome.*

## *3.2 Flowchart*

Flowchart digunakan untuk menggambarkan urutan langkah-langkah dan aliran logis dari suatu proses atau algoritme. Simbol-simbol tersebut dihubungkan dengan panah yang menunjukkan aliran dari satu langkah ke langkah berikutnya. Flowchart dapat membantu dalam memahami, merancang, dan menganalisis proses atau algoritme secara visual. Mereka juga dapat digunakan untuk menjelaskan langkah-langkah kepada orang lain dengan cara yang lebih jelas dan terstruktur.

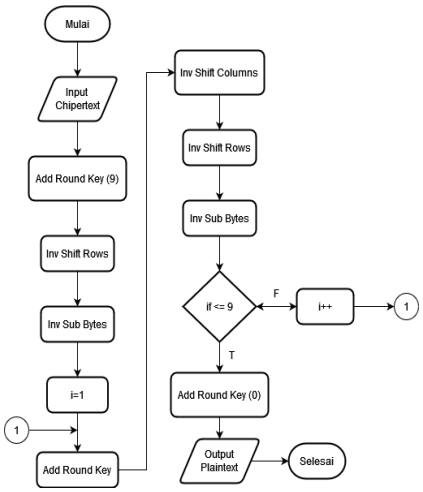
a. Flowchart proses enkripsi




**Gambar 4.** Flowchart Proses Enkripsi

Pada **gambar 4** Flowchart enkripsi AES 128 menggambarkan langkah-langkah yang harus diikuti untuk mengenkripsi blok data dengan menggunakan kunci enkripsi 128-bit. Tahap-tahap *SubBytes, ShiftRows, MixColumns, dan AddRoundKey*diulang dalam putaran utama sebanyak 9 kali, diikuti oleh putaran terakhir yang sedikit berbeda.

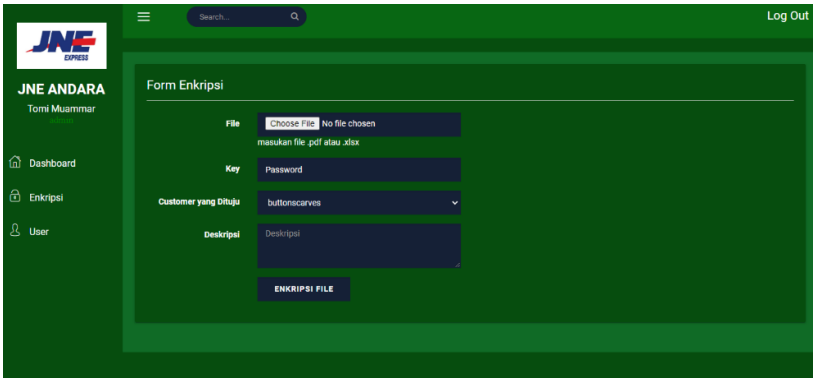
b. Flowchart proses dekripsi




**Gambar 5.** Flowchart Proses Dekripsi

Pada **gambar 5** Flowchart dekripsi AES menggambarkan langkah-langkah yang harus diikuti untuk mendekripsi blok data yang dienkripsi dengan menggunakan kunci dekripsi yang sesuai. Tahap-tahap *InvShiftRows, InvSubBytes, AddRoundKey, dan InvMixColumns* diulang dalam putaran utama sebanyak 9 kali, diikuti oleh putaran terakhir yang sedikit berbeda.

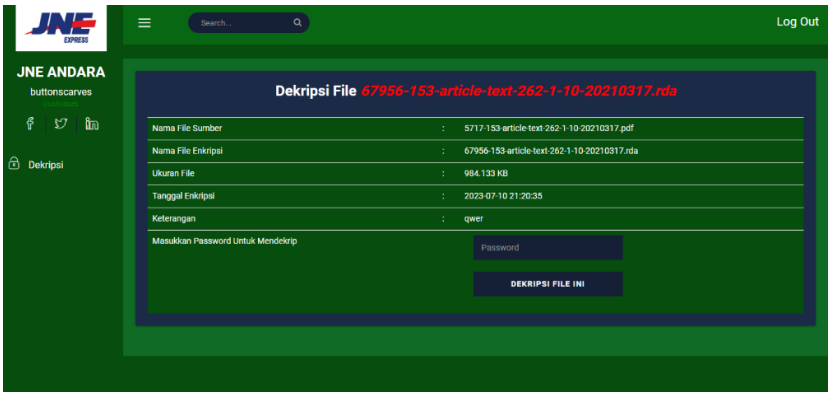
## 3.3 Tampilan Layar Halaman Enkripsi




**Gambar 6.** Tampilan Layar Halaman Enkripsi

Pada **gambar 6** di atas ini merupakan tampilan layar menu enkripsi, dimana dihalaman menu enkripsi ini pengguna dapat men enkripsi *file* yang memiliki *extension* tertentu seperti (.xlsx ,dan .pdf. ) kemudian pengguna di haruskan terlebih dahulu memasukan *(key) password* dan Deskripsi sebelum melakukan proses enkripsi.

### 3.4 Tampilan Layar Halaman Dekripsi

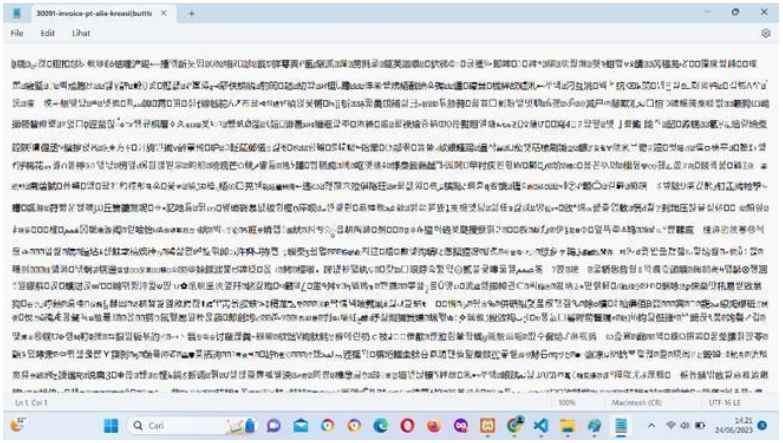



**Gambar 7.** Tampilan Layar Halaman Dekripsi

Pada **gambar 7** diatas adalah tampilan deskripsi berkas, pengguna bisa langsung mendeskripsi berkas yang sudah di enkripsi sebelumnya, tekan tombol deskripsi dan masukan password sesuai pada saat pengguna mengenkripsi berkas jika password valid maka deskripsi berkas akan berhasil dan jika tidak pengguna harus memasukkan ulang password dengan benar.

### 3.5 Tampilan *File* Setelah Di Enkripsi

Pada gambar gambar di bawah ini menampilkan hasil dari *file* asli yang telah di enkripsi, berikut tampilan *file* setelah di enkripsi

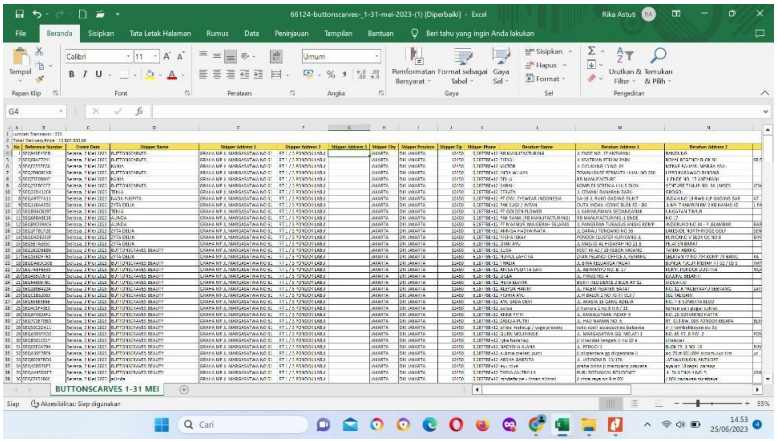


**Gambar 8.** Tampilan File Setelah Di Enkripsi

Pada **gambar 8** merupakan tampilan file setelah di enkripsi Tampilan sebuah file setelah dienkripsi akan bergantung pada algoritma enkripsi yang digunakan. Enkripsi merupakan proses mengubah data asli menjadi bentuk yang tidak terbaca dan hanya dapat dibaca kembali dengan menggunakan kunci dekripsi yang sesuai.

### 3.6 Tampilan *File* Setelah Di Dekripsi

Pada gambar gambar di bawah ini menampilkan hasil dari *file* yang telah di dekripsi, *file* yang telah di dekripsi akan kembali seperti *file* aslinya, berikut tampilan *file* setelah di dekripsi



**Gambar 9.** Tampilan *File* Setelah di Dekripsi

Pada **gambar 9** Tampilan file setelah didekripsi akan kembali ke bentuk aslinya sebelum dienkripsi. Proses dekripsi mengembalikan data yang sudah dienkripsi menjadi bentuk semula menggunakan kunci dekripsi yang sesuai.

## 3.7 Pengujian

Pengujian aplikasi merupakan proses penelitian untuk mendapatkan informasi tentang hasil yang dapat dilakukan oleh sistem aplikasi pengamanan *file* pada agen JNE Andara. Penulis ini melakukan 2 proses pengujian , yaitu pengujian proses enkripsi *file* dan pengujian proses dekripsi *file*. Berikut adalah contoh tabel pengujian dari enkripsi dan deskripsi program AES .

a. Hasil Pengujian Enkripsi

**Tabel 3.** Tabel Hasil Pengujian Enkripsi

| No | Nama File Awal | Ukuran File | Nama File Hasil Enkripsi | Ukuran File Setalah Enkripi | Status | |
|---|---|---|---|---|---|---|
| | | | | | Durasi Enkripi | Keterangan |
| 1 | 06juni-aliakreasi.xlsx | 15.9 KB | 50021-06juni-aliakreasi.rda | 15.9KB | 0.59 detik | Berhasil |
| 2 | 05juni-aliakreasi.xlsx | 16.7 KB | 44849-05juni-aliakreasi.rda | 16.7KB | 0.41 detik | Berhasil |
| 3 | Buttonscarves1-31 mei 2023.xlsx | 108 KB | 250070-buttonscarves 1-31 mei 2023.rda | 108 KB | 2.52 detik | Berhasil |
| 4 | Invoice-pt alia kreasi(buttonscarves ).pdf | 74.9 KB | 30091-invoice-pt alia kreasi.rda | 74.9KB | 1.71 detik | Berhasil |
| 5 | Transaksi 1juni-aliakreasi.xlsx | 587 KB | 1443-transaksi 1juni aliakreasi.rda | 587 KB | 13.64 detik | Berhasil |

Pada **tabel 3** Tabel hasil pengujian enkripsi biasanya digunakan untuk mencatat hasil dari uji coba atau eksperimen terhadap algoritma enkripsi yang berbeda atau parameter yang berbeda. Tujuan dari tabel ini adalah untuk memantau performa dan keamanan algoritma enkripsi dalam berbagai skenario.

b . Hasil Pengujian Dekripsi

**Tabel 4.** Tabel Hasil Pengujian Dekripsi

| No | Nama File Enkripsi | Ukuran File Enkripsi | Nama File Hasil Dekripsi | Ukuran File Dekripsi | Status | |
|---|---|---|---|---|---|---|
| | | | | | Durasi Enkripsi | Keterangan |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 50021-06juni-aliakreasi.rda | 15.9KB | 47256-06-juni---alia-kreasi.xlsx | 15.9KB | 0.5 detik | Berhasil |
| 2 | 44849-05juni-aliakreasi.rda | 16.7KB | 22737-05-juni---alia-kreasi-.xlsx | 16.7KB | 0.41 detik | Berhasil |
| 3 | 250070-buttonscarves-1-31mei-2023.rda | 108 KB | 66124buttonscarves_1-31-mei 2023.xlsx | 108 KB | 2.5 detik | Berhasil |
| 4 | 30091-invoice-pt aliakreasi(buttonscarves).rda | 74.9KB | 54584-invoice-pt-alia-kreasi(buttonscarves).pdf | 74.9KB | 1.7 detik | Berhasil |
| 5 | 1443-transaksi-1juni-aliakreasi.rda | 587 KB | 77731-transaksi-1juni-aliakreasi.xlxs | 587 KB | 13 detik | Berhasil |

Pada **tabel 4** Tabel hasil pengujian dekripsi mencatat hasil dari uji coba atau eksperimen terhadap proses dekripsi data yang sebelumnya telah dienkripsi. Ini membantu untuk memantau seberapa baik algoritma dekripsi dan kunci dekripsi bekerja dalam mengembalikan data ke bentuk semula.

## 4. KESIMPULAN

Berdasarkan analisis yang telah dilakukan terhadap permasalahan dan pengujian dari berbagai analisis yang telah dilakukan terhadap permasalahan pada aplikasi yang telah dikembangkan, disimpulkan bahwa aplikasi pengamanan data pengiriman customer pada Agen JNE Andara menggunakan teknik kriptografi dengan metode *Advanced Encryption Standard* (AES 128) mampu menjaga keamanan data pengiriman dalam *file* dokumen sehingga dapat mencegah potensi kebocoran data. Adapun, ukuran file yang diproses mempengaruhi durasi yang ditempuh dalam proses enkripsi dan dekripsi tergantung pada ukuran *file* dokumen yang akan diproses. Dimana semakin minim ukuran pada file yang akan di proses, semakin cepat juga encryption (enkripsi) dan (decryption) dekripsi, dan semakin tinggi/besar ukuran file, maka semakin lama enkripsi dan dekripsi.

## DAFTAR PUSTAKA

[1] F. Akbar and S. Waluyo, “SISTEM KEAMANAN DATABASE MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD(AES-128) STUDI KASUS : RED AVENUE INDONESIA”, *SKANIKA*, vol. 1, no. 2, pp. 821-828, May 2018.

[2] J. Handoyo and Y. M. Subakti, ‘KEAMANAN DOKUMEN MENGG UNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES)’, 2020. [Online]. Available: http://www.jurnal.umk.ac.id/sitech

[3] D. Nurnaningsih and A. A. Permana, ‘RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCYPTION STANDARD (AES)’, *JURNAL TEKNIK INFORMATIKA*, vol. 11, no. 2, pp. 177–186, Nov. 2018, doi: 10.15408/jti.v11i2.7811.

[4] T. H. L. Sodikin, ‘"Analisa Keamanan E-Commerce Menggunakan Metode Aes Algoritma,” Teknokom, vol. 3, no. 2, pp. 8–13, 2020’.

[5] I. Priambudi, ‘Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa’, *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 6, no. 1, p. 22, 2023.

[6] O. G. Khoirunnisa and D. Djuniadi, ‘Implementasi Algoritma AES untuk Keamanan Data Rekam Medis’, *PETIR*, vol. 15, no. 1, pp. 21–27, Dec. 2021, doi: 10.33322/petir.v15i1.1333.

[7] F. Diny Hermawati and M. Tahir, ‘Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advance Encryption Standard)’, Pendidikan Informatika, 2023.

[8] 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’, *Applied Information System and Management (AISM)*, vol. 3, no. 2, pp. 69–78, Jan. 2021, doi: 10.15408/aism.v3i2.14722.

[9] M. Azhari, J. Perwitosari, and F. Ali, ‘Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi *Advanced Encryption Standard* (AES)’, *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1390.

[10] R. Nuari and N. Ratama, ‘Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping’, 2020. [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA

[11] D. Widyawan and 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.

[12] N. Sijabat, N. Hayaty, E. Suswaini, M. Raja, and A. Haji, ‘IMPLEMENTASI KRIPTOGRAFI HYBRID MENGGUNAKAN ALGORITMA AES-128 DAN ALGORITMA RABIN UNTUK MENGAMANKAN DATA

DALAM DATABASE'.2022

[13] W. Nur Cholifah and S. Melati Sagita, 'PENGUJIAN BLACK BOX TESTING PADA APLIKASI ACTION & STRATEGY BERBASIS ANDROID DENGAN TEKNOLOGI PHONEGAP', 2018.