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

IMPLEMENTASI *ALGORITME* KRIPTOGRAFI METODE *AES-128* UNTUK PENGAMANAN *FILE* LAPORAN DATA PENJUALAN PADA MAKEMA *COFFEE*

Muhammad Rizki[1*], Sejati Waluyo[2]

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

Email: [1*]1911502258@student.budiluhur.ac.id, [2]sejati.waluyo@budiluhur.ac.id
(* : corresponding author)

Abstrak- Dalam perkembangan digitalisasi masa kini, semua kebutuhan manusia sangat membutuhkan inovasi teknologi diantaranya dapat menerapkan pengamanan data, dari data informasi yang umum maupun rahasia. Dengan maraknya pencurian dari berbagai macam bentuknya oleh karena itu sangatlah memerlukan kerangka kerja yang diharapkan untuk mendapatkan pengamanan sebuah *file* atau data, sangat berguna untuk melindungi data, maka sangat memungkinkan tidak ada pihak yang tidak bertanggung jawab melakukan pencurian data penting. Salah satu *algorime* untuk pengamanan data berupa *file* yaitu dikenal dengan nama Kriptografi, Kriptografi adalah salah satu dari berbagai metode enkripsi yang digunakan untuk mengamankan data. Metode ini melibatkan proses penyandian pesan dengan mengubah susunan huruf-huruf dari pesan asli menggunakan aturan tertentu, sehingga isi pesan hanya bisa dipahami oleh sekelompok orang tertentu yang memiliki kunci yang tepat. Makema *Coffee* adalah kedai kopi yang menjual berbagai macam jenis minuman yang sangat dinikmati banyak kalangan. Makema *Coffee* memiliki laporan yang sangat penting, misalnya informasi transaksi secara konsisten, dan keamanan catatan data penjualan ini harus dijaga dengan baik. guna tidak disalah gunakan oleh pihak yang tidak berkepentingan. Tentang masalah ini, dan tentang rencana penelitian ini merakit Sistem keamanan, ini berfungsi untuk melindungi data berupa berkas dokumen dengan menggunakan metode enkripsi - dekripsi menggunakan Teknik Kriptografi *AES-128.* Kriptografi merupakan seni mengubah pesan agar sulit dilacak. Standar Enkripsi Lanjutan (AES) merupakah salah satu *algoritme* enkripsi yang digunakan. Selain itu, kunci acak midsquare juga efektif dalam menjaga keutuhan keamanan seluruh berkas.

Kata Kunci: Kriptografi, *AES-128,* Dokumen, Enkripsi, Dekripsi.

IMPLEMENTATION OF THE AES-128 METHOD CRYPTOGRAPHIC ALGORITHM TO SECURE SALES DATA REPORT FILES AT MAKEMA COFFEE

Abstract- *In today's digitalization development, all human needs really need technological innovation, including being able to implement data security, from general and confidential information data. With the rise of theft of various forms, therefore it is very necessary to have a framework that is expected to get the security of a file or data, very useful for protecting data, it is very possible that no irresponsible party steals important data. One of the algorithms for securing data in the form of files is known as Cryptography, Cryptography is one of the various encryption methods used to secure data. This method involves the process of encoding a message by changing the arrangement of the letters of the original message using certain rules, so that the contents of the message can only be understood by a certain group of people who have the right key. Makema Coffee is a coffee shop that sells various types of drinks that are enjoyed by many people. Makema Coffee has very important reports, such as consistent transaction information, and the security of these sales data records must be properly maintained so that they are not misused by unauthorized parties. About this problem, and about this research plan to assemble a security system, this serves to protect data in the form of document files using the encryption - decryption method using the AES-12 Cryptographic Technique.*

***Keywords*:** *Cryptography, AES-128, Document, Encryption, Decryption.*

1. PENDAHULUAN

Dengan cepatnya perkembangan inovasi dalam bidang data dan komunikasi, memungkinkan banyak orang untuk saling bertukar informasi, termasuk *file* data atau data yang bersifat rahasia. Oleh karena itu, penting untuk menjaga keamanan informasi tersebut supaya tidak ada individu yang tidak memiliki hak dapat membaca,

mengubah, atau menghapusnya. Salah satu cara untuk mencapai keamanan informasi adalah dengan menggunakan Teknik Kriptografi, yang melibatkan teknik enkripsi dan dekripsi.

Kriptografi berasal dari bahasa Yunani, menggabungkan dua elemen kata, yaitu "kripto" yang merujuk pada pengubahan menjadi rahasia, dan "graphia" yang mengacu pada cara menulis atau mencatat.Di dalam bidang kriptografi, terdapat persamaan matematika yang digunakan untuk melakukan enkripsi dan dekripsi data [1]. Secara umum, perhitungan kriptografi gaya lama dibagi menjadi dua *klasifikasi*, yaitu kode *interpretasi* khusus dan angka pengganti. [2].

Kriptografi adalah salah satu dari berbagai metode enkripsi yang digunakan untuk mengamankan data. Metode ini melibatkan proses penyandian pesan dengan mengubah susunan huruf-huruf dari pesan asli menggunakan aturan tertentu, sehingga isi pesan hanya bisa dipahami oleh sekelompok orang tertentu yang memiliki kunci yang tepat. Terdapat dua jenis *algoritme* kriptografi berdasarkan kunci enkripsi dan dekripsi *Algoritme simetris*, juga dikenal sebagai *algoritme* kriptografi konvensional, menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Sementara itu, *algoritme asimetris* menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. [3].

Algoritme Advanced Encryption Standard (AES) adalah sebuah *algoritme block cipher* yang memiliki sifat *simetri*, artinya ia menerapkan kunci identik saat melakukan langkah pengamanan dan pengembalian informasi yang terenkripsi [4]. *AES-128* adalah *algoritme block cipher* yang menentukan sifat keseragaman *block cipher* Menerapkan kunci yang sama pada kedua sisi dalam proses mengamankan dan mengembalikan informasi. Teknik enkripsi lanjutan (AES) melibatkan transformasi terhadap state dalam beberapa *ronde* untuk mencapai pengamanan data [5]. Pada umumnya, siklus enkripsi adalah *AES-128* dengan kunci *128-bit* [6]. Data dapat disandikan dan dipulihkan kembali menjadi bentuk semula menggunakan *algoritme AES* dengan Ukuran kunci dapat berupa 128, 192, atau 256 bit. Dimensi kunci ini berpengaruh terhadap jumlah putaran yang dijalankan dalam langkah-langkah enkripsi dan dekripsi. [7]. Secara sederhana, *algoritme* dekripsi *AES* adalah kebalikan dari *algoritme* enkripsi AES [5]. *SubBytes* (Transformasi Substitusi *Byte*), *ShiftRow* (Transfornasi Pergeseran Baris), *MixColumns* (Transformasi Percampuran Kolom), *AddRoundKey* (Transformasi Penambahan Kunci) [8]. *Random Key Midsquare* adalah metode perhitungan yang digunakan untuk menghasilkan angka acak. Metode ini berguna untuk mengacak angka kunci. [9].

Penelitian sebelumnya yang ada di Indonesia telah membahaas enkripsi kriptografi dengan metode *AES-128* berbasis android [10]. dengan judul "*Implementasi Algoritme AES 128 BIT* Sebagai Pengamanan Teks Di Aplikasi *Note Berbasis Android*" pada penelitian ini kegunaannya untuk mengamankan teks berupa catatan berbasis *androi*d menggunakan metode *AES-128 bit* pada aplikasi *note*.

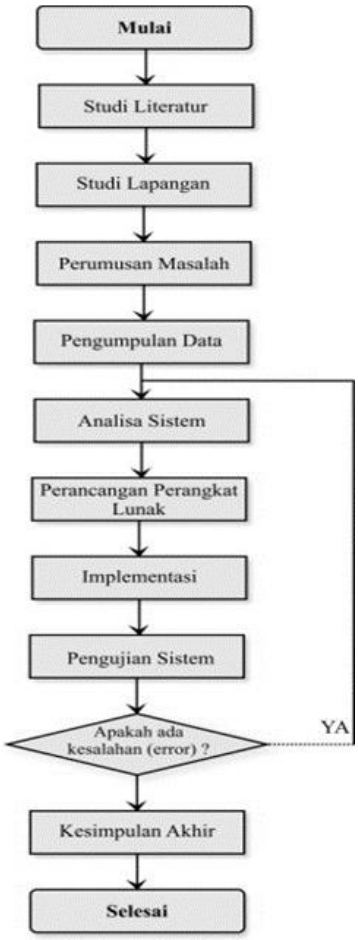
Makema *Coffee*, yang terletak di *JL. DR SOETOMO, CILEDUG TANGERANG*, merupakan tempat yang populer untuk bersantai dengan suasana yang menarik, baik dalam ruangan maupun di luar ruangan, dengan sentuhan estetika yang menawan. Oleh karena itu, Makema *Coffee* menjadi pilihan bagi berbagai kalangan untuk berkumpul, baik untuk rapat atau sekadar bersantai bersama teman atau keluarga. Dengan menu yang beragam dan layanan yang baik, Makema *Coffee* bertujuan untuk memuaskan hati dan menyenangkan para pelanggan.

Makema *Coffee* memiliki dokumen penting, khususnya data penjualan setiap bulan, yang sangat rahasia karena berisi informasi tentang keuntungan dan kerugian bisnis. Maka dari itu, data transaksi ini dijaga dengan baik dengan tujuan agar tidak disalahgunakan. Untuk mengatasi masalah ini, muncul pemikiran untuk merencanakan kerangka kerja keamanan yang dapat melindungi informasi sebagai dokumen, dengan memanfaatkan strategi kriptografi *AES-128*. Motivasi untuk menggunakan *Advanced Encryption Standard (AES)* adalah karena *algoritme* ini bekerja pada *128-bit* atau 16-karakter, yaitu memungkinkan enkripsi teks dengan keamanan yang tinggi.

Terkait dari permasalahan diatas, sebagai Tindakan pencegahan maka akan dilakukan penerapan untuk mengamankan *file-file* penting dengan menggunakan kriptografi. Penelitian ini menggunakan kriptografi metode *Advance Encryption Standard 128* yang bertujuan untuk mengamankan filenya terutama *file* berukuran <*3mb* yang berformat *doc,txt,pdf,xlsx*.

2. METODE PENELITIAN

Pada langkah ini berperan sebagai pemandu untuk menjalankan eksplorasi ini, memastikan hasil yang diperoleh terus berada pada jalur yang telah ditetapkan sebelumnya. Simak gambaran tentang teknik yang tergambar dalam gambar 1, menggambarkan tahapan-tahapan di mana metodologi penelitian diterapkan dalam penyelidikan ini.



Gambar 1. Metodelogi Penelitian

2.1 Studi Literatur

Pada fase ini, investigasi terhadap beberapa perangkat dan ide yang akan kami manfaatkan dalam penelitian yang telah selesai. Pelengkapan penelitian ini juga diselesaikan melalui telaah mendalam terhadap 10 *papper jurnal* dari tahun 2019 sampai dengan tahun 2023. dan artikel logis tentang hal yang diperiksa, khususnya kriptografi metode enkripsi *Advanced Encryption Standard (AES).*

2.2 Perumusan Masalah

Ketika melangkah ke tahap ini, perbincangan akan berpusat pada permasalahan yang hendak dijelajahi, yakni penelusuran tentang cara melindungi laporan data penjualan yang ada di dalam Makema *Coffee.* Dimana akan menerapkan teknik enkripsi yang dikenal sebagai *Advance Encryption Standard (AES-128).*

2.3 Pengumpulan Data

Ketika sampai pada fase ini, dari seluruh data yang telah dijelaskan sebelumnya. Semua langkah dalam proses pengumpulan data didasarkan pada pertemuan dan kesepahaman mengenai informasi yang diperlukan.

a. Wawancara *(interview)*

Mengadakan rapat dengan semua pihak terkait. Dalam upaya menciptakan sebuah aplikasi yang mengupas tuntas informasi terkait aspek keamanan yang ada.

b. Observasi *(observation)*

Observasi adalah metode bermacam-macam informasi yang sukses untuk menyelidiki, di mana hal ini dapat dicapai dengan mendeteksi secara langsung teknik atau proses yang sedang berjalan.

2.4 Analisa Sistem

Pada fase Ini merupakan langkah di mana kita mencari dan mengupas masalah yang muncul dalam sistem, semuanya disesuaikan dengan kendala-kendala yang ada. Dalam upaya mengenali masalah ini, analisis yang dijalankan diharapkan mampu menjadi solusi yang dapat mengatasi masalah dalam penelitian ini. Langkah-langkah yang ditempuh mencakup analisis data, evaluasi penerapan algoritme, serta tinjauan mendalam terhadap kerangka sistem.

2.5 Perancangan Perangkat Lunak

Ketika memasuki tahap ini, kita merampungkan tahapan perancangan dengan memanfaatkan hasil kajian sistem, khususnya rancangan modul enkripsi dan dekripsi serta pendukung lainnya, nantinya akan dikordinasikan dalam aplikasi, Model ini mensyaratkan bahwa satu Langkah harus diselesaikan dengan baik sebelum menlanjutkan Menuju langkah selanjutnya, dan capaian dari tiap langkah haruslah tercermin dengan jelas dan *factual.*

2.6 Implementasi

Dalam siklus pengimplementasian disinilah segmen yang disusun pada proses ini penyusunan dibuat dalam Bahasa pemerograman spesifik tertentu. Perangkat lunak yang digunakan selama menjalankan proses keamanan informasi dokumen menggunakan Bahasa pemrograman Aplikasi manajemen basis data yang terpilih adalah *PHP My Admin.* Adapun mesin-mesin perkakas yang diterapkan melibatkan otak Intel *Core i7,* daya memorinya mencapai 16 gigabita, dan jantungnya adalah *SSD* berkapasitas *256 giga.*

2.7 Tahap Pengujian Sistem

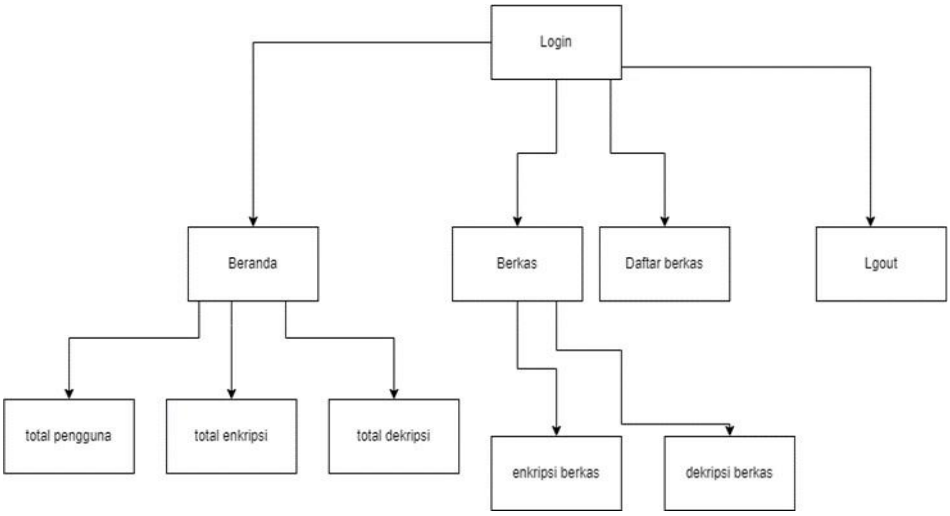
Tahap pengujian sistem, tujuannya adalah Menyakinkan bahwa sistem yang telah dikerjakan sejalan dengan output yang diidentifikasi dan direncanakan sehingga dapat menciptakan sebuah hasil akhir yang sejajar dengan tujuan yang diharapkan. Oleh karena itu, penting untuk melakukan strategi pengujian yang mencakup Tindakan atau Batasan agar dapat menguji sistem dengan *rasionalitas* sehingga dapat *memverifikasi* apakah sistem berjalan sebagaimana yang diharapkan.

2.8 Rancangan Menu

Program ini menghadirkan sejumlah Jendela yang akan dihasilkan, termasuklah Jendela masuk, Jendela tampilan utama, serta Jendela Berkas yang menyediakan Subjendela untuk langkah enkripsi-dekripsi. Ketika pertama kali masuk, langkah awal adalah menjalani proses login dengan mengisi username dan kata sandi sebelum memasuki tahap berikutnya di dalam aplikasi.

Untuk melindungi berkas, terdapat submenu khusus enkripsi di dalam jendela berkas, di mana pengguna diharuskan mengisi detail yang diperlukan seperti berkas yang hendak dienkripsi (tetapi tidak melebihi batas kapasitas aplikasi), memasukkan kata sandi, serta opsi dekripsi. Setelah tahap ini, pengguna dapat meneruskan langkah enkripsi dengan menetapkan berkas yang ingin dienkripsi.

Selanjutnya, untuk memulihkan dokumen yang telah dienkripsi, pengguna dapat memilih submenu Dekripsi dari jendela Berkas. Di sini, pengguna memiliki opsi untuk menentukan status dekripsi dan akan diarahkan ke berkas data yang akan didekripsi. Pengguna akan diharuskan memasukkan kata sandi untuk menginisiasi dekripsi dan memilih berkas yang hendak didekripsi. Setelah langkah-langkah ini, program akan menjalankan proses untuk mengembalikan data ke bentuk aslinya, yang dapat dilihat dalam ilustrasi pada Gambar 2.



Gambar 2. Rancangan Menu

2.9 Kesimpulan

Pada puncak perjalanan ini, diambil kesimpulan mengenai penerapan Teknik Enkripsi *Advance Encryption Standard (AES)* guna melindungi berkas, dengan mengambil acuan dari hasil uji coba yang telah dijalankan untuk memastikan bahwa penggunaan Teknik Enkripsi *Advance Encryption Standard (AES)* dapat menjaga keutuhan dokumen dengan tepat. Selain itu, dalam tahap ini juga muncul gagasan-gagasan untuk penyempurnaan aplikasi ini di masa depan.

3. HASIL DAN PEMBAHASAN

Bab ini merangkum pelaksanaan praktis program kriptografi untuk berkas dokumen *berformat web*, seperti **.doc, *.xls, *.docx, *.xlsx, *.ppt, dan *.txt,* dengan menerapkan teknik *AES-128.* Selain itu, bagian ini mendetail dengan bantuan gambar dan tabel yang menggambarkan langkah-langkahnya. juga akan menyingkap kebutuhan spesifik baik dari perangkat lunak maupun perangkat keras yang terlibat dalam proses ini.

3.1 Lingkungan percobaan

Persyaratan teknis untuk menjalankan aplikasi perlu memenuhi kriteria agar operasional aplikasi berjalan sesuai yang diinginkan. Rincian teknis di bawah ini memastikan sistem ini berjalan dengan lancar:

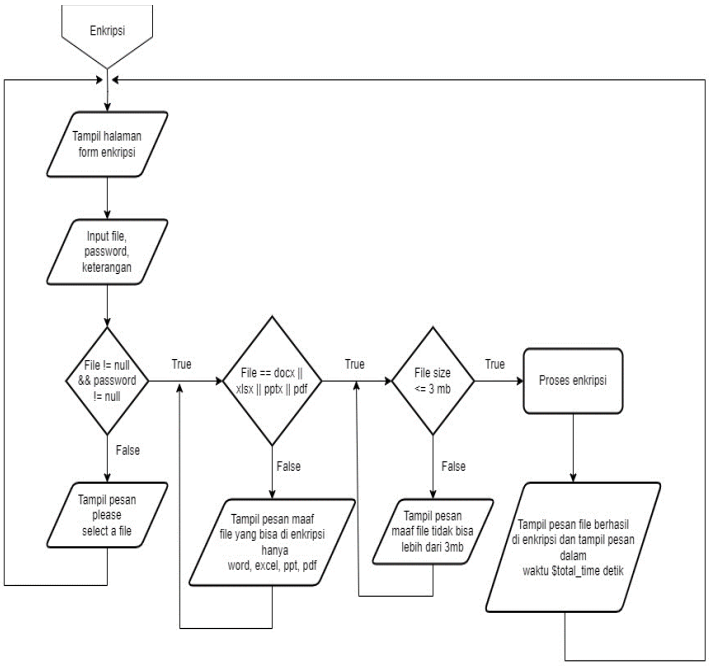
a. Komponen perangkat lunak yang digunakan dalam pelaksanaan aplikasi mencakup beberapa elemen, yakni Sistem Operasi Windows 11, XAMPP Control Panel v3.2.2, Microsoft Office 2021, Google Chrome, dan MYSQL.
b. Sementara itu, kelengkapan perangkat keras yang digunakan untuk mengimplementasikan aplikasi ini terdiri dari, prosesor Intel(R) Core(T) i7-8265U berkecepatan 1.60GHz hingga 1.80GHz, memori RAM sebesar 16GB, laptop berkapasitas penyimpanan solid-state 477GB.

3.2 *Flowchart*

Berbagai rangkaiaan proses yang harus dilalui dijelaskan pada bagian *format flowchart* diikuti dengan *Flowchart* dan *Algoritme* setiap prosesnya, dengan adanya *flowchart* juga membantu untuk perencanaan dan mengoptimalkan algoritme, sehingga proses ini dapat berjalan dengan lebih efesien dan efektif, tercangkup pada pernyataan berikut:

3.2 *Flowchart* Halaman *Enkripsi File*

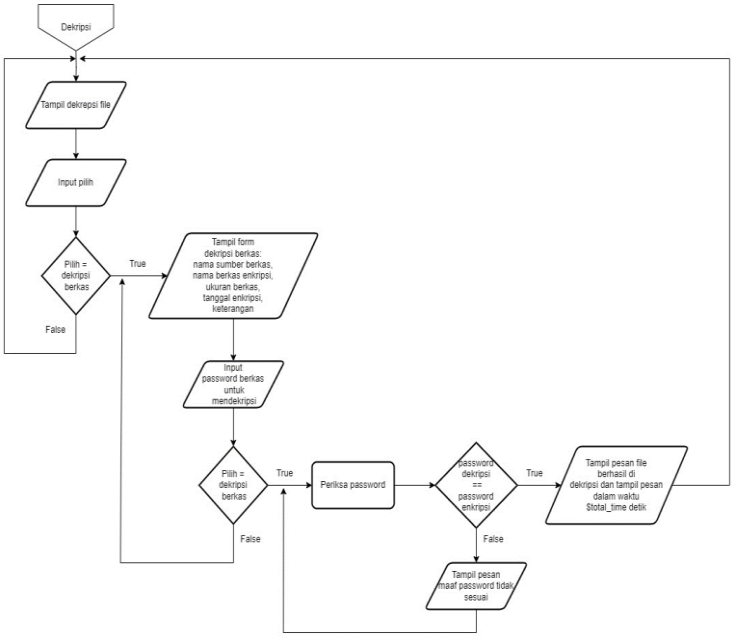
Flowchart halaman enkripsi *file* (proses enkripsi). Di dalamnya ada dua pilihan bagian, yakni penyandian dan penyusunan kembali sandi (enkripsi-dekripsi), yang terlihat jelas pada Ilustrasi 3. Ini adalah gambaran rencana ilustrasi alur dari jendela menu berkas khusus langkah penyandian.yang dimana *admin* akan melakukan proses pengenkripsian *file* dengan melakukan *upload file* dan mengisi *password.* Lalu *file* yang akan di input yaitu *file* yang *berformat *.doc, *.xls, *.docx, *.xlsx, *.ppt, *. dan *.txt* dan ukuran *file* tidak bisa lebih dari 3mb.



Gambar 3. *Flowchart* Halaman Enkripsi *File*

3.3 *Flowchart* Halaman Dekripsi *File*

Flowchart halaman dekripsi *file (*proses dekripsi). Di dalamnya tersedia 2 opsi bagian, yaitu penyandian dan pemulihan sandi, bisa diintip pada gambar 4. ini adalah rancangan *flowchart menu file* halaman dekripsi. Yang dimana admin akan melakukan proses pendekrisian *file* dimana *file* yang sudah dienkripsi akan dikembalikan lagi ke *file* yang aseli, yaitu dengan memilih *file* yang akan didekripsi, jika sudah memilih *file* yang akan didekripsi *admin* akan memasukan *password file* tersebut guna memproses dekripsi *file* supaya *file* tersebut Kembali ke bentuk yang asli.



Gambar 4. *Flowchart* Halaman Dekripsi *File*

3.4 Pengujian Program

Proses selanjutnya yaitu menguji aplikasi yang sudah selesai dibuat. Dalam fase Ini dapat dijelaskan dalam hal pengujian aplikasi enkripsi dan dekripsi. Tes tersebut nantinya akan menghasilkan enkripsi dari *file* yang akan dienkripsi. Dan kecepatan mengukur kecepatan *file* ketika dienkripsi atau ketika didekripsi.

3.5 Proses Enkripsi

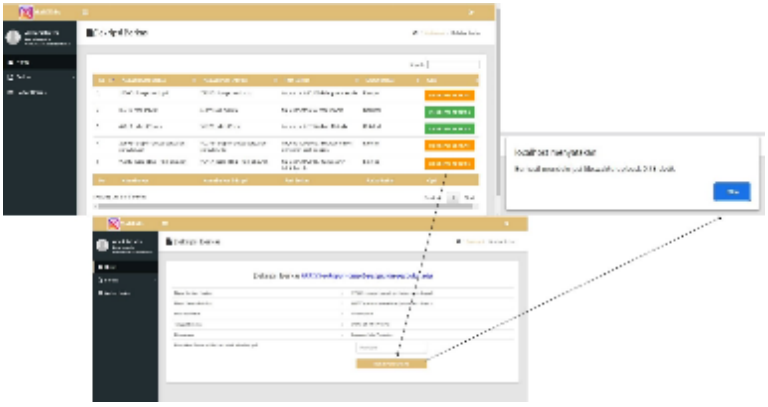
Langkah awal ialah mengakses laman penyandian atau halaman enkripsi dan memilih berkas yang diniatkan untuk dijaga kerahasiaannya. Setelah itu, langkah berikutnya adalah menyusupkan kata sandi serta keterangan terhadap berkas yang direncanakan untuk disandikan. Setelah berhasil, tampilan *pop-up* pemberitahuan keberhasilan akan muncul. Sementara pada tahap lanjutan, langkah pertama tetap sama dengan memilih berkas yang akan dijaga, serta memberikan kata sandi dan keterangan, seperti yang diilustrasikan pada gambar 5. Kemudian, ke tombol "enkripsi berkas". Bila tindakan pengenkripsian berhasil, maka layar *pop-up* akan segera menyapa. Gambar 6 hasil enkripsi, dimana *file* yang sebelumnya dapat dibaca berubah menjadi kode *file* yang tidak dapat dibaca.

Gambar 5. Proses Enkripsi *File*

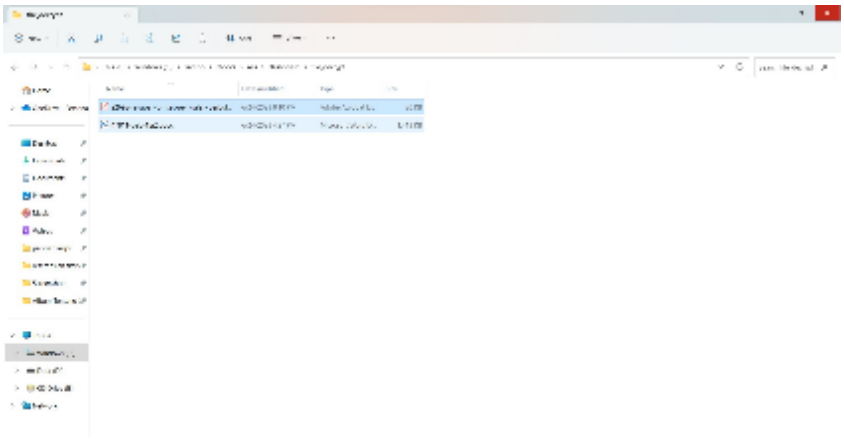
Gambar 6. Hasil Enkripsi *File*

3.6 Proses Dekripsi

Bagi yang ingin mengembalikan berkas yang telah dirahasiakan atau mereset kembali sandi, langkahnya cukup sederhana. Cukup menuju Jendela Dekripsi Berkas, lalu pilihlah berkas yang ingin didekripsi. Setelah itu, cukup klik tombol “DEKRIPSI BERKAS”. Langkah berikutnya akan muncul tampilan seperti pada Gambar 7 dan 8. Untuk terus memproses dekripsi, pengguna akan diminta untuk memasukkan kata sandi yang sama seperti yang diterapkan pada berkas yang telah dienkripsi sebelumnya. Bila kata sandi yang diinput benar, sebuah kotak pesan *pop-up* akan muncul sebagai pemberitahuan sukses.



Gambar 7. Proses Dekripsi *File*



Gambar 8. Hasil Dekripsi File

3.7 Hasil Pengujian Enkripsi dan Dekripsi *File*

Inilah hasil dari eksperimen yang telah dijalankan pada aplikasi Enkripsi dan Dekripsi *AES-128*, dengan tujuan untuk mengetahui sejauh mana hasilnya sukses atau sebaliknya. Tabel 1 menggambarkan capaian dari pengujian Enkripsi yang dilakukan dalam konteks aplikasi Enkripsi dan Dekripsi *AES-128*.

Table 1. Hasil Pengujian Enkripsi

Dokumen				Status	
No	**Nama File**	**Aseli**	**Hasil Enkripsi**	**Enkripsi**	**Waktu**
1	REKAPAN OMSET PENJUALAN PERBULAN.pdf	30 kb	30 kb	BERHASIL	0,64 Detik

Sementara itu, di Tabel 2, kita temukan hasil uji coba Dekripsi pada program Enkripsi dan Dekripsi AES-128.

Table 2. Hasil Pengujian Dekripsi

Dokumen				Status	
No	**Nama File**	**Aseli**	**Hasil Dekripsi**	**Dekripsi**	**Waktu**
1	REKAPAN OMSET PENJUALAN PERBULAN.pdf	30 kb	30 kb	BERHASIL	0,64 Detik

4. KESIMPULAN

Setelah menguraikan masalah yang dijelaskan pada bagian-bagian dan aplikasi sebelumnya, dapat diambil kesimpulan bahwa program aplikasi keamanan laporan data penjualan untuk Makema *Coffee* menggunakan metode *Advance Encryption Standard (AES-128).* aplikasi kriptografi ini berfungsi sebagai langkah pengamanan data dari potensi serangan oleh pihak yang tidak bertanggung jawab. Setelah *file* terenkripsi, hanya sistem yang dapat membukanya. Dengan kata lain, *file* tersebut tidak dapat dibuka dengan aplikasi lain untuk mengurangi risiko penyalahgunaan oleh pihak yang tidak berkepentingan. Lalu pepmbuatan *program* pengamanan *file* dengan metode *algoritme AES-128* telah berhasil diimplementasikan dalam bentuk *website* dan *program* sehingga ini dapat berguna untuk mengamankan data *berformat *.doc, *.xls, *.docx, *.xlsx, *.ppt, *. dan *.txt*. Namun, *program* enkripsi dan dekripsi ini memiliki beberapa keterbatasan dan kekurangan.

Selanjutnya pencipta mengusulkan beberapa saran untuk meningkatkan aplikasi ini agar *program* dapat dipikirkan dan lebih unggul di kemudian hari. Di harapkan *program* ini dapat diperbaiki untuk menghadapi *file* yang lebih besar dari *3mb,* dan mengembangkan kembali sistem pengamanan *file* ini agar tidak hanya mengamankan *file berformat *.doc, *.xls, *.docx, *.xlsx, *.ppt, *. dan *.txt*.

DAFTAR PUSTAKA

[1] 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.

[2] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Jurnal Pendidikan Sains dan Komputer Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) Jurnal Pendidikan Sains dan Komputer," vol. 2, no. 1, pp. 163–171, 2022.

[3] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan Php," *J. Teknol. Inf.*, vol. 1, no. 1, p. 11, 2019, doi: 10.36294/jurti.v1i1.21.

[4] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *JIKOMSI [Jurnal Ilmu Komput. dan Sist. Informasi]*, vol. 4, no. 2, pp. 75–85, 2021, [Online]. Available: https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

[5] L. Mustika, "Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 148, 2020, doi: 10.30865/jurikom.v7i1.1943.

[6] 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.

[7] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan the Implementation of Advanced Encryption Standard on the Encryption and Decryption of the Confidential Documents At," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020.

[8] M. Imron and A. Pratama, "Pengamanan E-Dokumen Berbasis Steganografi Dengan Kombinasi Advanced Encryption Standard (AES) 128 Bit," *InfoTekJar*, vol. 6, no. 2, pp. 6–10, 2022.

[9] F. Mahbub, M. Syahrizal, and R. K. Hondro, "Modifikasi Kunci Algoritma IDEA Menggunakan Random Key Midsquare Pada Citra," vol. 2, no. 12, pp. 204–210, 2020, doi: 10.30865/komik.v4i1.2681.

[10] A. Permana and E. Jaelani, "Implementasi Algoritma AES 128 Bit sebagai Pengaman Teks di Aplikasi Note Berbasis Android," *JEJARING J. Teknol. dan …*, vol. 5, no. November, pp. 9–17, 2020, [Online]. Available: https://journal.uniku.ac.id/index.php/jejaring/article/view/6716%0Ahttps://journal.uniku.ac.id/index.php/jejaring/article/viewFile/6716/3272