SENAFTI
SEMINAR NASIONAL MAHASISWA
FAKULTAS TEKNOLOGI INFORMASI

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

PENERAPAN KRIPTOGRAFI MENGGUNAKAN METODE AES UNTUK PENGAMANAN DATA PENJUALAN RUMAH MAKAN MITRA MINANG

Ilham Wahyu Kuncoro Aji[1*], Reva Ragam Santika[2]

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

Email: [1*]1911510798@student.budiluhur.ac.id, [2]reva.ragam@builuhur.ac.id
(* : corresponding author)

Abstrak-Seiring dengan meningkatnya penggunaan teknologi informasi dalam industri restoran, keamanan data menjadi prioritas utama, terutama dalam data nota transaksi. Rumah Makan Mitra Minang, yang mengandalkan sistem pembayaran *online* maupun *offline*, menghadapi tantangan signifikan terkait dengan keamanan data transaksi. Untuk mengatasi risiko kebocoran atau penyalahgunaaan data transaksi dari akses yang tidak sah dari orang yang tidak bertanggung jawab, maka diterapkannya metode kriptografi AES 128 (*Advanced Encryption Standard*) yaitu, sebuah algoritma enkripsi dekripsi simetris yang diakui secara luas karena tingkat keamanan dan efisiensinya. Penerapan AES pada sistem transaksi Rumah Makan Mitra Minang melibatkan data transaksi pembayaran, yang mencakup informasi pribadi pelanggan, serta data transaksi lainnya. Dengan itu maka metode AES ini sangat diperlukaan untuk menambah pengamanan pada data transaksi. Implementasi ini meliputi integrasi AES ke dalam arsitektur sistem transaksi, yang mencakup proses enkripsi data transaksi dan dekripsi saat data transaksi diterima. Pada hasil pengujian sistem yang dibuat menunjukkan bahwa pada penerapan metode AES secara signifikan meningkatkan keamanan data transaksi dengan mengurangi potensi risiko pencurian data dari serangan siber maupun dari pihak yang tidak bertanggung jawab. Dengan sistem yang dilindungi oleh AES, Rumah Makan Mitra Minang dapat memastikan bahwa data pelanggan yaitu transaksi tetap aman, meningkatkan kepercayaan pelanggan serta mematuhi standar keamanan data yang berlaku. Studi ini menegaskan pentingnya adopsi teknologi kriptografi dalam menjaga integritas dan kerahasiaan informasi dalam industri restoran.

Kata Kunci: *Advanced Encryption Standard (AES)*, Kriptografi, Enkripsi, Dekripsi

IMPLEMENTATION OF CRYPTOGRAPHY USING THE AES METHOD FOR SECURING SALES DATA AT MITRA MINANG RESTAURANT

Abstract- *As the use of information technology in the restaurant industry increases, data security becomes a top priority, especially in transaction note data. Mitra Minang Restaurant, which relies on online and offline payment systems, faces significant challenges related to transaction data security. To overcome the risk of leakage or misuse of transaction data from unauthorized access by irresponsible people, the AES 128 (Advanced Encryption Standard) cryptography method is implemented, namely a symmetric encryption decryption algorithm that is widely recognized for its level of security and efficiency. The application of AES to the Mitra Minang Restaurant transaction system involves payment transaction data, which includes customer personal information, as well as other transaction data. With that, the AES method is very much needed to increase security in transaction data. This implementation includes the integration of AES into the transaction system architecture, which includes the process of encrypting transaction data and decrypting it when the transaction data is received. The results of testing the system that was created showed that the application of the AES method significantly increased the security of transaction data by reducing the potential risk of data theft from cyber attacks or from irresponsible parties. With a system protected by AES, Rumah Makan Mitra Minang can ensure that customer data, namely transactions, remains safe, increasing customer trust and complying with applicable data security standards. This study emphasizes the importance of adopting cryptographic technology in maintaining the integrity and confidentiality of information in the restaurant industry. emphasizes the importance of adopting cryptographic technology in maintaining the integrity and confidentiality of information in the restaurant industry.*

Keywords*: Advanced Encryption Standard (AES), Cryptography, Encryption, Decryption*

1. PENDAHULUAN

Dengan berkembang semakin cepat, teknologi informasi memiliki dampak positif dan negatif. Kemajuan teknologi dapat menyebabkan penyalahgunaan data, yang merupakan salah satu dampak negatifnya. Oleh karena itu, keamanan dan kerahasiaan data perusahaan sangat penting pada masa kini. Masalah keamanan dan kerahasiaan data merupakan salah satu masalah yang paling penting. Data dapat berupa dokumen digital seperti *Microsoft word*, *PDF*, dan *excel*, serta nota pembelian dan penjualan. Dan maka ada kemungkinan hal yang tidak diinginkan

akan terjadi jika pihak yang tidak bertanggung jawab mencoba mengakses atau mengubah data tersebut. Oleh karena itu, dibutuhkan suatu aplikasi yang dapat melindungi data, termasuk nota pembelian dan penjualan [1].

Suatu usaha UMKM (Usaha Mikro Kecil dan Menengah) yang berbasis di Jakarta adalah Rumah Makan Mitra Minang. Penyalah gunaan data nota penjualan dan pembelian hasil transaksi oleh individu yang tidak bertanggung jawab dapat berdampak negatif pada pelanggan. Untuk menjaga kerahasiaan dan keamanan data atau nota, sistem keamanan kriptografi *Advanced Encryption Standard* (AES) dibuat. Rumah Makan Mitra Minang menghadapi banyak masalah, salah satunya adalah kurangnya keamanan yang memadai terhadap informasi pekerja yang dapat menyebabkan akses ilegal dan pelanggaran privasi yang dapat merugikan bisnis perushaan dan para pegawai. Tujuan dari penelitian ini ialah untuk dapat mengimplementasikan algoritma AES 128 dengan sukses pada *platform* enkripsi berbasis web dan meningkatkan keamanan *file* yang berisi data pada nota transaksi pelanggan [2].

Menurut buku-buku yang telah pernah diterbitkan sebelum tahun 1980-an, kriptografi ialah suatu seni dan ilmu dalam hal untuk bisa agar menjaga kerahasiaan suatu pesan dengan merahasiakannya ke dalam bentuk yang tidak mudah dapat dibaca dan ditafsirkan kembali. Kriptografi juga mencakup studi metode matematika yang erat berkaitan dalam aspek suatu keamanan informasi seperti kerahasiaan, integritas, dan otentikasi [3]. Algoritma AES 128 merupakan algoritma enkripsi simetris yang mendekripsi dan mengenkripsi pesan dengan kunci 128-bit [4]. Meskipun panjang kunci algoritma AES bervariasi, ukuran bloknya tetap 128 bit. Algoritma ini melibatkan sejumlah perulangan yang disebut "*round*", yang terdiri dari sepuluh putaran, saat menggunakan kunci AES-128. Matriks empat kali empat berukuran satu byte atau delapan bit digunakan untuk melakukan operasi enkripsi dan dekripsi dalam setiap putaran [5].

Penelitian ini memilih algoritma AES sebagai temuan penelitian sebelumnya yang menunjukkan bahwa AES masih memiliki kecepatan untuk pada proses enkripsi dan dekripsi yang lebih tinggi daripada beberapa metode algoritma lain yang pernah diuji [6]. Pada penelitian sebelumnya oleh Azhari et al. dengan judul " Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritma Kriptografi *Advanced Encryption Standard (AES)"* [7]. Karena ukuran data AES lebih kecil dan kecepatan pada proses enkripsi yang lebih cepat dari metode kriptografi lainnya jadi, peneliti menggunakan metode AES-128 untuk membuat aplikasi berbasis web [8].

2. METODE PENELITIAN

2.1 Keamanan Informasi Data

Keamanan data mencakup menjaga data digital dan nondigital dari akses, penggunaan, atau pengungkapan yang tidak sah sesuai dengan strategi risiko perusahaan. Selain itu, ini melindungi data dari gangguan, perubahan, atau penghancuran. Keamanan data sangat penting untuk menjaga data organisasi tetap rahasia, jujur, dan tersedia karena data sangat penting bagi kehidupan setiap organisasi dan keberhasilan perusahaan. Dengan menerapkan langkah-langkah keamanan data yang kuat, perusahaan dapat memenuhi persyaratan kepatuhan, menjaga kepercayaan pelanggan, dan melindungi aset berharga mereka [2]. Komponen aman dimaksudkan untuk mencegah data komputer jatuh ke tangan orang yang tidak berhak. *Password* digunakan untuk meningkatkan keamanan komputer dengan mencegah orang yang tidak berhak mengakses data pribadi (rahasia), mencegah data dimanipulasi atau dirusak (integritas), dan memberi tahu orang yang berhak mengakses data [9].

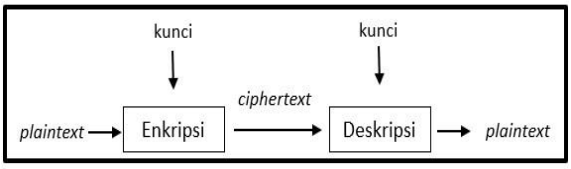
2.2 Kriptografi

Kriptografi adalah proses mengkodekan atau menyembunyikan data sehingga hanya orang yang dimaksud dapat membacanya. Kriptografi telah digunakan untuk mengkodekan pesan selama ribuan tahun. Kata sandi komputer, kartu bank, dan e-commerce masih menggunakannya. Sandi dan algoritma yang digunakan dalam alat kriptografi modern memungkinkan enkripsi dan dekripsi data, seperti kunci enkripsi 128-bit dan 256-bit. Sandi modern, seperti Standar Enkripsi Tinggi (AES), dianggap tidak dapat dipecahkan. Kriptografi, juga dikenal sebagai kriptologi, adalah metode keamanan siber yang menggunakan kode informasi untuk menjamin bahwa hanya orang yang menerima pesan yang dapat membaca dan memprosesnya. Teknik ini menggunakan ilmu komputer, teknik, dan matematika untuk membuat kode kompleks yang menyembunyikan makna sebenarnya dari pesan [10]. Didalam kriptografi sering menggunakan berbagai istilah atau terminologi. Ada beberapa macam istilah yang harus dipahami, yaitu :

a. *Cipherteks*, *plainteks*, dan pesan adalah teks terenkripsi yang dilindungi data pengguna dengan algoritma enkripsi. Teks terenkripsi tidak dapat dibaca sebelum diubah kembali menjadi teks asli melalui proses enkripsi, di mana kunci yang disebut *cipher* [10].

b. Pengirim atau penerima adalah komunikasi yang melibatkan suatu pertukaran pada pesan dengan dua atau lebih. Pengirim *(sender)* adalah orang yang mengirim pesan kepada penerima lainnya. Penerima *(receiver*) adalah orang yang menerima pesan [11].
c. Enkripsi dan dekripsi ialah proses mengubah data atau informasi yang akan dikirim untuk menjadi bentuk yang tidak dikenal dengan mengubah informasi menggunakan algoritma tertentu. Kebalikan dari enkripsi, dekripsi ialah mengubah kembali informasi kedalam bentuk semula menjadi informasi awal [12].
d. *Cipher* dan kunci adalah suatu algoritma kriptografi yang sangat penting yang digunakan pada *plaintext* atau informasi tertentu untuk mengubahnya menjadi teks *cipher*. Selain itu, *cipher* diperlukan untuk mengubah teks *cipher* menjadi teks plain yang dapat dibaca dan dipahami oleh pihak yang terlibat dalam informasi. Tanpa *cipher*, penerima informasi tidak akan dapat memahami teks *cipher* [11].

Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci algoritma tidak lagi dirahasiakan, tetapi kunci tetap dirahasiakan. Parameter yang digunakan untuk enkripsi dan dekripsi adalah kunci. Secara umum, kunci terdiri dari *string* atau deretan bilangan. Fungsi enkripsi dan dekripsi dapat ditulis dengan kunci K seperti yang ditunjukkan pada Gambar 1.



Gambar 1. Kunci dengan skema enkripsi dan dekripsi

2.3 *Advanced Encryption Standard* AES

Untuk keamanan data, *Advanced Encryption Standard* (AES) ialah suatu metode algoritma kriptografi yang terdiri dari blok *chipertext* simetrik yang mudah digunakan untuk mengenkripsi dan mendekripsi. Enkripsi mengubah data sehingga tidak dapat mudah dibaca, dan dekripsi mengubah data ke format aslinya, yang dikenal sebagai *plaintext*. Dengan kunci kriptografi 128, 192, dan 256 bits, algoritma AES mengenkripsi dan mendekripsi data pada blok 128 bits. Jumlah proses yang perlu dilakukan untuk enkripsi dan dekripsi bergantung pada ukuran blok data dan kunci. Dibawah ini adalah tabel AES pada tabel 1.

Tabel 1. Jumlah proses yang teridiri dari bit blok dan kunci

Panjang Kunci Dalam bit	Panjang Kunci (Nk) Dalam words	Ukuran Blok Data (Nb) Dalam words	Jumlah Proses (Nr)
128	4	4	10
192	6	4	12
256	8	4	14

2.4 Rancangan Pengujian

Pengujian dilakukan dalam beberapa langkah untuk memastikan bahwa setiap fitur elemen aplikasi bekerja dengan baik.Di bawah ini ialah rancangan pengujian pada tebel 2.

Tabel 2. Rancangan Pengujian

Kelas Uji	Detail Pengujian	Jenis Pengujian
Login admin atau pegawai	Memverifikasi *data login admin* dan pegawai dengan memasukan *username* dan *password*	*Black box*
Pengujian enkripsi *file*	Proses enkripsi mengupload data dengan memilih data yang ingin di upload lalu memasukan *password* beserta deskripsi keterangan	*Black box*

Kelas Uji	Detail Pengujian	Jenis Pengujian
Pengujian dekripsi *file*	Proses dekripsi dengan memasukan *password* yang sama pada *file* yang dienkripsi	*Black box*
Pengujian penambahan pegawai	Proses pendaftaran dengan memasukan *username*, *password*, nama, pekerjaan, dan status. Sekaligus proses simpan	*Black box*

2.5 Rancangan Basis Data

Untuk menjalankan aplikasi, basis data yang mengandung semua data diperlukan pada tahap proses ini. Desain basis data digambarkan dalam tabel 3 untuk tabel pengguna dan tabel 4 untuk tabel file.

Primary Key : *username*
Isi : data *user*

Tabel 3. Rancangan basis data users

No	Nama	Tipe Data	Keterangan
1	*username*	varchar(15)	*username*
2	*password*	varchar(15)	*password*
3	*fullname*	varchar(50)	nama *user*
4	*job_title*	varchar(50)	pekerjaan
5	status	enum(1,2)	status pengguna

Primary Key : id_file
Isi : Data *file*

Tabel 1. Rancangan basis data *file*

No	Nama	Tipe Data	Keterangan
1	*id_file*	int(11)	*id_file*
2	*username*	varchar(15)	*username*
3	*file_name_source*	varchar(255)	nama *file* asli
4	*file_name_finish*	varchar(255)	nama *file* hasil
5	*file_url*	varchar(255)	*url file*
6	*file_size*	float	ukuran *file*
7	*password*	varchar(16)	*password*
8	status	enum(1,2)	status pengguna
9	keterangan	varchar(255)	keterangan

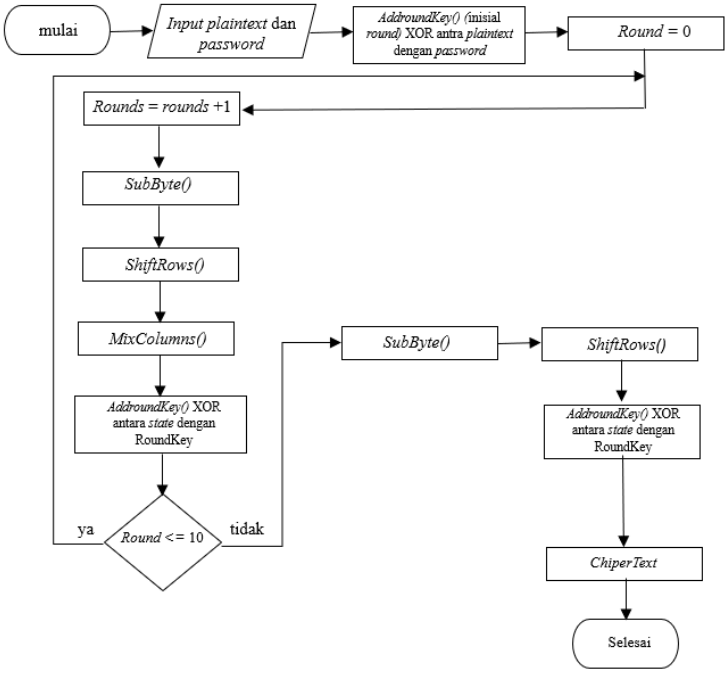
3. HASIL DAN PEMBAHASAN

3.1 *Flowchart*

Program ini berfokus dalam menu yang memungkinkan pengguna mengenkripsi algoritma AES, ada proses enkripsi yang melibatkan empat macam jenis perubahan *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Pada tahap pertama enkripsi, input yang telah disalin pada bagian state akan menerima byte *AddRoundKey*. Selanjutnya, input ke bagian *state* akan menerima perubahan *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara terus-menerus sejumlah *Nr*. Proses ini juga dikenal sebagai *round function* dalam algoritma AES. Program ini berfokus pada menu yang memungkinkan pengguna mengenkrisi dan mendekripsi dokumen.

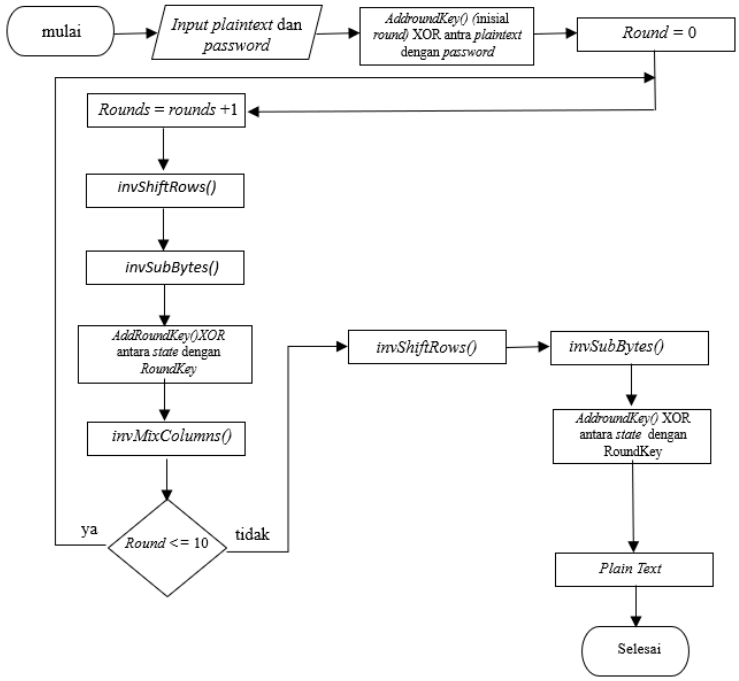
Ini memungkinkan pemilik data agar dapat melindungi dokumen pengguna dengan metode enkripsi dan dekripsi AES 128.

Pada gambar 2, menunjukkan *flowchart* proses enkripsi. Proses enkripsi menggunakan algoritma kriptografi AES 128 bit dimulai dengan *key expansion*, yaitu memperluas kunci enkripsi 128 bit menjadi serangkaian *sub* kunci yang akan digunakan dalam setiap putaran enkripsi. Pada putaran awal, blok *plaintext* 128 bit di *XOR* dengan kunci pertama yang dihasilkan dari ekspansi kunci. Selanjutnya, terdapat 9 putaran utama yang masing-masing terdiri dari empat langkah. Langkah pertama adalah *SubBytes*, di mana setiap byte dalam blok *plaintext* digantikan dengan byte lain menggunakan *S-Box* (*substitution box*). Langkah kedua adalah *ShiftRows*, di mana baris-baris dalam blok digeser secara sirkular ke kiri, dengan jumlah pergeseran yang berbeda untuk setiap baris. Setelah itu, pada langkah *MixColumns*, setiap kolom dalam blok dimodifikasi melalui operasi matematika yang mengkombinasikan nilai setiap byte dalam kolom tersebut. Langkah terakhir dari setiap putaran adalah *AddRoundKey*, di mana hasil dari langkah sebelumnya di *XOR* dengan *sub* kunci berikutnya yang dihasilkan dari *key expansion*. Pada putaran akhir, hanya tiga langkah yang dilakukan, yaitu *SubBytes*, *ShiftRows*, dan *AddRoundKey*, tanpa melibatkan *MixColumns*. Setelah seluruh proses selesai, hasil akhir yang diperoleh adalah *ciphertext* 128 bit yang telah dienkripsi.



Gambar 2. *Flowchart* tahapan proses pada enkripsi

Pada Gambar 3, menunjukkan *flowchart* proses untuk dekripsi. Proses dekripsi menggunakan algoritma AES 128 bit adalah kebalikan dari proses enkripsinya. Langkah pertama dimulai dengan *key expansion*, di mana kunci dekripsi dihasilkan dari kunci asli melalui proses ekspansi kunci. *Sub* kunci yang dihasilkan akan digunakan secara terbalik selama proses dekripsi. Pada putaran awal, *ciphertext* 128 bit di *XOR* dengan *sub* kunci terakhir yang dihasilkan dari ekspansi kunci. Selanjutnya, terdapat 9 putaran utama yang terdiri dari empat langkah. Pertama adalah *InvShiftRows*, di mana baris-baris dalam blok digeser secara sirkular ke kanan dengan jumlah pergeseran yang sama seperti dalam enkripsi, tetapi arah sebaliknya. Kedua adalah *InvSubBytes*, di mana setiap byte dalam blok digantikan dengan byte lain menggunakan invers dari *S-Box*. Setelah itu, pada langkah *AddRoundKey*, hasil dari langkah sebelumnya di *XOR* dengan *sub* kunci yang sesuai dari *key expansion*. Langkah keempat adalah *InvMixColumns*, dimana setiap kolom dalam blok dimodifikasi menggunakan operasi matematika yang merupakan kebalikan dari *MixColumns* selama enkripsi. Pada putaran akhir, hanya tiga langkah yang dilakukan, yaitu *InvShiftRows*, *InvSubBytes*, dan *AddRoundKey*, tanpa melibatkan *InvMixColumns*. Setelah seluruh proses selesai, hasil akhirnya adalah *plaintext* 128 bit yang telah berhasil dikembalikan ke bentuk semula, sesuai dengan teks asli sebelum enkripsi.



Gambar 3. *Flowchart* tahapan proses pada dekripsi

3.2 Tampilan Layar

a. Tampilan Layar Proses *Login*

Pada gambar 4, menjelaskan tahap tampilan *login* aplikasi enkripsi dan dekripsi rumah makan mitra minang pada saat pertama kali dibuka, ini juga merupakan menu awal di halaman *login* untuk memasukkan *username* dan password masing-masing pengguna *admin* dan pegawai.

Gambar 4. Menu halaman *login admin* dan pegawai

b. Tampilan Layar Halaman *Dashboard*

Pada gambar 5, menjelaskan apabila pengguna *admin* berhasil *login* setelah itu akan masuk kedalam menu utama yaitu menu *dashboard*. Pada menu *dashboard* ini berada dihalaman utama pada aplikasi ini. Pada pengguna *admin* terdadapat 4 menu utama yaitu, hasil keseluruhan, unggah *file* (enkripsi *file* dan dekripsi *file*), dan pegawai.

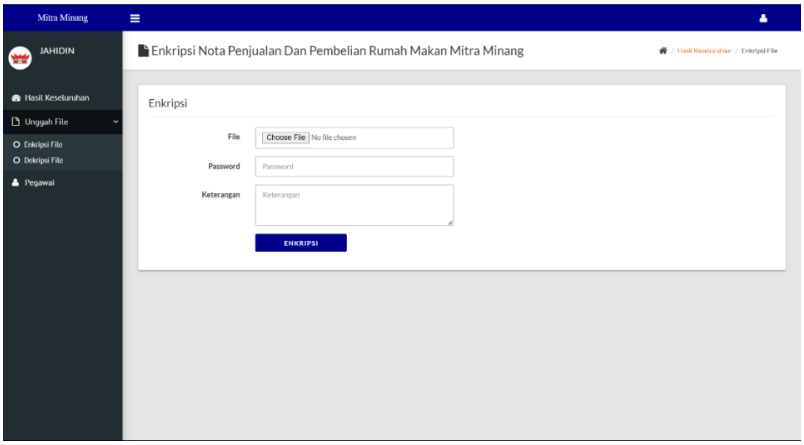
Gambar 5. Menu Halaman Awal *Admin*

Sedangkan pada gambar 6, menjejelaskan apabila pengguna pegawai berhasil *login* setelah itu akan masuk kedalam menu utama yaitu menu *dashboard.* Pada menu *dashboard* ini berada dihalaman utama pada aplikasi ini. Pada pengguna *admin* hanya terdadapat 3 menu utama yaitu, hasil keseluruhan, unggah *file* (enkripsi *file*).

Gambar 6. Menu Halaman Awal Pegawai

c. Tampilan Layar Halaman Enkripsi *Admin* dan Pegawai

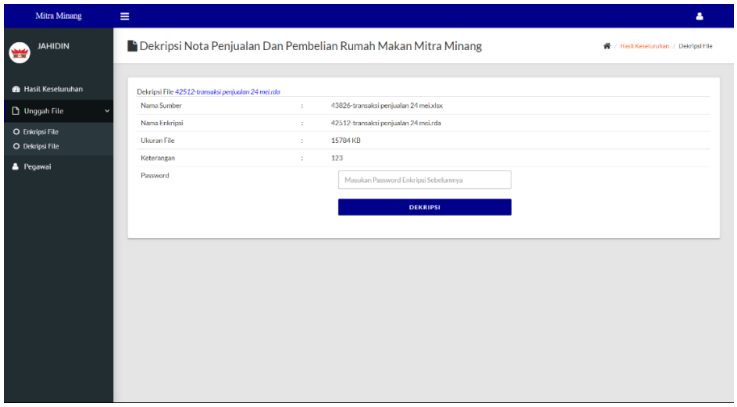
Pada gambar 7, submenu ini digunakan untuk mengenkripsi *file* dengan ukuran tidak lebih dari 2 MB saja dimana hanya file yang berbentuk docx, pdf, xlsx, dan pptx serta jpg. Disini pengguna diminta untuk memilih *file* yang telah disiapkan untuk dienkripsikan. Setelah itu pengguna wajib mengisi *password* dan keterangan.



Gambar 7. Menu Halaman Enkripsi *Admin* Dan Pegawai

d. Tampiilan Layar Halaman Dekripsi *Admin*

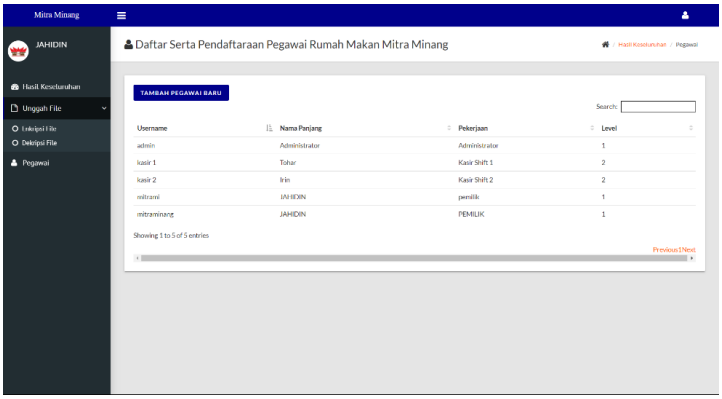
Pada gambar 7, Selanjutnya pada *submenu* dekripsi *admin* yang digunakan untuk menampilkan kembali *file* yang telah dienkripsikan, pada *submenu* ini terdapat menu atau tombol "dekripsi*"* disamping kanan pada *file* yang telah dienkripsi. Setelah itu menu akan menampilkan lanjutan pada proses untuk mendekripsikan *file* dengan memasukan *password* yang telah diisi sesuai *file* yang telah dienkripsikan sebelumnya.



Gambar 7. Menu Halaman Dekripsi *Admin*

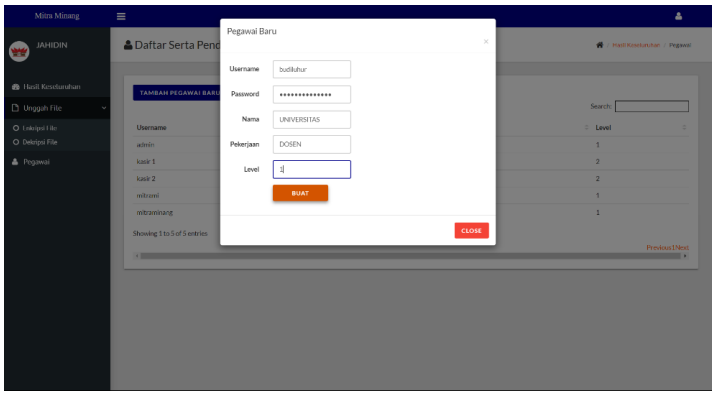
e. Tampiilan Layar Halaman menu pegawai *admin*

Pada gambar 8, menjelaskan pada tahap menu ini bertujuan untuk melihat daftar karyawan atau pegawai yang sudah terdaftar.



Gambar 8. Menu Halaman Pegawai Pada *Admin*

Sedangkan gambar 9, menjelaskan submenu pada menu pegawai untuk penambahan karyawan atau pegawai baru, dengan cara mengklik menu "Tambah Pegawai Baru" Selanjutnya akan muncul *popup* untuk mengisi *Username, Password*, Nama, Pekerjaan, dan Status. Selanjutnya tinggal klilk "BUAT".



Gambar 9. Menu halaman Proses Tambah Pegawai

3.3 Hasil Pengujian Pada Enkripsi dan Dekripsi *File*

Pada tabel 5 menunjukkan hasil pengujian enkripsi untuk program pada aplikasi enkripsi dekripsi.

Tabel 5. Hasil uji coba enkripsi

No	Nama *File*	Ukuran *File*	Waktu Dibutuhkan
1	transaksi penjualan 21 mei (xlsx)	15 KB	3.52 detik
2	transaksi penjualan 24 mei (xlsx)	15 KB	3.50 detik
3	pembelian bahan 1 (pdf)	87,1 KB	5.14 detik
4	Pembelian bahan 2(pdf)	103 KB	5.91 detik
5	Contoh penjualan 1 (jpg)	53 KB	3.27 detik
6	Contoh pembelian bahan 1 (jpg)	100 KB	5.68 detik
7	Contoh *file* (docx)	12 KB	1.16 detik
8	Contoh *file* (pptx)	35 KB	2.37 detik
9	Contoh *file* (xlsx)	11 KB	1.11 detik
10	Uji coba *file* 2 MB	2 MB	1 menit 41 detik

Pada tabel 6 menunjukkan hasil pengujian dekripsi untuk program aplikasi enkripsi dekripsi.

Tabel 6. Hasil uji coba dekripsi

No	Nama *File*	Ukuran *File*	Waktu Dibutuhkan
1	transaksi penjualan 21 mei (xlsx)	15 KB	2.67 detik
2	transaksi penjualan 24 mei (xlsx)	15 KB	2.59 detik
3	Pembelian bahan 1 (pdf)	87,1 KB	3.88 detik
4	Pembelian bahan 2 (pdf)	103 KB	4.45 detik
5	Contoh penjualan 1 (jpg)	53 KB	2.62 detik
6	Contoh pembelian bahan 1 (jpg)	100 KB	4.21 detik
7	Contoh *file* (docx)	12 KB	1.30 detik
8	Contoh *file* (pptx)	35 KB	1.95 detik
9	Contoh *file* (xlsx)	11 KB	0.91 detik
10	Uji coba *file* 2 MB	2 MB	1 menit 41 detik

Pada penelitian ini bertujuan untuk mengevaluasi seberapa efektif implementasinya. Dengan melihat hasil pada kedua tabel diatas, dan dapat diartikan bahwa dari hasil tabel pengujian enkripsi *file* dan dekripsi *file* dengan menggunakan berbagai macam *extension*, seperti docx, pptx, xlsx, pdf, dan jpg yang telah dilakukan diatas disimpulkan bahwa ukuran dari suatu *file* yang ingin dienkripsi maupun didekripsikan sangat mempengaruhi waktu proses yang dibutuhkan, semakin kecil suatu ukuran *file* yang ingin dienkripsi dan didekripsikan maka waktu yang dibutuhkan sangatlah singkat dan sebaliknya apabila *file* yang ingin dienkripsi dan didekripsikan cukup besar maka waktu proses yang dibutuhkan sangatlah relatif lama.

4. KESIMPULAN

Setelah melakukan penelitian ini AES 128 dapat disimpulkan bahwa, pada Rumah Makan Mitra Minang telah berhasil mengimplementasikan aplikasi kriptografi AES 128 berbasis web untuk dapat mengamankan data transaksi penjualan maupun pembelian. Dalam pengujian yang dilakukan tampak bahwa, waktu yang digunakan pada saat melakukan sebuah proses enkripsi dan proses dekripsi sangat berbanding lurus pada ukuran *file* yang

akan diproses. Dengan ini, jika ukuran *file* saat proses enkripsi maupun dekripsi itu kecil maka proses waktu yang dibutuhkan relatif singkat, sebaliknya apabila saat ukuran file tersebut besar maka waktu yang dibituhkan saat proses enkripsi maupun dekripsi berjalan relatif lebih lama. Dan ukuran *file* saat proses enkripsi dan dekripsi tidak mengalami perubahan.

Untuk membuat keamanan data yang akan dilakukan agar lebih aman dan tidak dapat diakses oleh orang yang tidak berkepentingan, pada penelitian selanjutnya dinantikan dapat menggabungkan lebih sempurna dan banyak menggunakan teknik kriptografi lainnya dalam satu pengamanan suatu *file*.

DAFTAR PUSTAKA

[1] Pramusinto, W., Wizaksono, N., & Saputro, A., "Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman," *BIT (Budi Luhur Information Technology)*, vol. 16, no. 2, pp. 47–53, 2019.

[2] Oktavani, S et al., "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *Jurnal Media Informatika*, vol. 4, no. 2, pp. 97-101, 2023.

[3] D. Widyawan and I. 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, doi:10.36080/skanika.v4i1.2216.

[4] R. D. Ardiya and W. Pramusinto, "Implementasi Algoritma Aes-128 Untuk Pengamanan Database Pada Sma Islamic Centre," *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi*, vol. 1, no. 1, September, 2022, pp. 93–102.

[5] 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.

[6] A. Ignasius, and D. V. S. Y. Sakti, "Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di PT. Gunung Geulis Elok Abadi," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 5, no. 1, pp. 1–10, 2022, doi:10.36080/skanika.v5i1.2118.

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

[8] Y. P. Putra, T. Mufizar, and E. Alfiyani, "Implementasi Super Enkripsi Aes Dan Rsa Pada Pengamanan Data Rekam Medis Pasien," *J. VOI (Voice of Informatic)*, vol. 11, no. 2, 37-46, 2022.

[9] Pratiwi, & WP, A. D. (2016). Peningkatan Keamanan Data dengan Metode Cropping Selection Pseudorandom. http://encoders-decoders.online-domain-tools.com.

[10] Lyman, C., 5 jenis metode enkripsi (chiper) dalam kriptografi, 2022. https://pintu.co.id/blog/jenis-enkripsi-cipher-kriptografi.

[11] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Jurnal Informatika Mulawarman*, vol. 10, no. 1, pp. 20-31, 2015.

[12] F. Muharram, H. Azis, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi*, vol. 3, no. 2, pp. 112-115, 2018.