

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

**TUGAS AKHIR**



**Oleh :**

**Ilham Wahyu Kuncoro Aji**

**NIM : 1911510798**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS BUDI LUHUR  
JAKARTA  
2024**

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

**Diajukan untuk memenuhi salah satu persyaratan memperoleh  
gelar Sarjana Komputer (S.Kom)**

**TUGAS AKHIR**



**Oleh:**

**Ilham Wahyu Kuncoro Aji**

**NIM : 1911510798**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS BUDI LUHUR**

**JAKARTA**

**2024**

## LEMBAR PENGESAHAN



PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS BUDI LUHUR

### LEMBAR PENGESAHAN



Nama : Ilham Wahyu Kuncoro Aji  
Nomor Induk Mahasiswa : 1911510798  
Program Studi : Teknik Informatika  
Bidang Peminatan : Programming Expert  
Jenjang Studi : Strata 1  
Judul : PENERAPAN KRIPTOGRAFI MENGGUNAKAN METODE AES UNTUK  
PENGAMANAN DATA PENJUALAN RUMAH MAKAN MITRA  
MINANG

Laporan Tugas Akhir ini telah disetujui, disahkan dan direkam secara elektronik sehingga tidak memerlukan tanda tangan tim penguji.

Jakarta, Senin 29 Juli 2024

Tim Penguji:

Ketua	: Purwanto, S.Si, M.Kom
Anggota	: Joko Christian Chandra, S.Kom., M.Kom.
Pembimbing	: Reva Ragam Santika, S.Kom., M.M., M.Kom
Ketua Program Studi	: Dr. Indra, S.Kom., M.T.I

## ABSTRAK

### **Penerapan Kriptografi Menggunakan Metode AES Untuk Pengamanan Data Penjualan Rumah Makan Mitra Minang**

**Oleh : Ilham Wahyu Kuncoro Aji (1911510798)**

Keamanan transaksi merupakan aspek krusial dalam bisnis restoran seperti Rumah Makan Mitra Minang. Penelitian ini bertujuan untuk meningkatkan keamanan data nota penjualan dan pembelian dengan menerapkan kriptografi, khususnya *Advanced Encryption Standard* (AES). Metode ini digunakan untuk mengenkripsi dan mendekripsi data transaksi pada nota penjualan dan pembelian, sehingga melindungi informasi sensitif dari akses yang tidak sah atau dari pihak yang tidak bertanggung jawab. Pada penelitian ini efektivitas implementasi AES dalam memperkuat keamanan data nota penjualan dan pembelian dengan mempertimbangkan aspek keamanan, efisiensi, dan keterjangkauan. Hasil penelitian menunjukkan bahwa penggunaan AES memberikan lapisan tambahan perlindungan terhadap informasi transaksi, meningkatkan kepercayaan kepada pemilik perusahaan dan mengurangi risiko kebocoran data. Implikasi praktis dari penelitian ini adalah memberikan panduan bagi Rumah Makan Mitra Minang dalam mengamankan data transaksi mereka dengan memanfaatkan teknologi kriptografi ini.

**Kata Kunci : Kriptografi, Enkripsi, dan AES**

x+53 halaman; 40 gambar; 11 tabel; 2 lampiran

## SURAT PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN PUBLIKASI

### SURAT PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN PUBLIKASI

Saya yang bertanda tangan dibawah ini :

Nama : Ilham Wahyu Kuncoro Aji  
NIM : 191510790  
Program Studi : Teknik Informatika  
Bidang Peminatan : Programming Expert  
Jenjang Studi : Strata 1  
Fakultas : Teknologi Informatika

Menyatakan bahwa TUGAS AKHIR yang berjudul:

Penerapan Kriptografi Menggunakan Metode AES Untuk Pengamanan Data Penjualan.....  
Rumah Makan Nitra Mirang.....

Merupakan :

1. Karya tulis saya sebagai laporan tugas akhir yang asli dan belum pernah diajukan untuk mendapatkan gelar akademik apapun, baik di Universitas Budi Luhur maupun di perguruan tinggi lainnya.
2. Karya tulis ini bukan saduran / terjemahan, dan murni gagasan, rumusan dan pelaksanaan penelitian / implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan pembimbing di organisasi tempat riset.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Saya menyerahkan hak milik atas karya tulis ini kepada Universitas Budi Luhur, dan oleh karenanya Universitas Budi Luhur berhak melakukan pengelolaan atas karya tulis ini sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh berdasarkan karya tulis ini, serta sanksi lainnya sesuai dengan norma di Universitas Budi Luhur dan Undang-Undang yang berlaku.

Jakarta, 29 Juli 2024  
  
Ilham Wahyu Kuncoro Aji

## **KATA PENGANTAR**

Puji dan Syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa Dengan mengucapkan Alhamdulillah dengan segala puji dan syukur penulis panjatkan atas kehadiran Allah SWT, karena berkat rahmat dan hidayahnya penyusunan Tugas Akhir yang berjudul “Penerapan Kriptografi Menggunakan Metode AES Untuk Pengamanan Data Penjualan Rumah Makan Mitra Minang” ini dapat diselesaikan untuk memenuhi persyaratan dalam menyelesaikan jenjang Strata Satu (S1) Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur.

Dalam pelaksanaan dan penyusunan skripsi ini dibuat dengan observasi dan bantuan dari berbagai pihak untuk menyelesaikan penyusunannya. Penulis menyadari bahwa laporan ini tidak mungkin terselesaikan tanpa adanya dukungan, bantuan, bimbingan dan nasehat dari berbagai pihak. Pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang setulus-tulusnya kepada :

1. Allah Subhanahu Wa Ta'ala, yang selalu memberikan rahmat disetiap langkah, nikmat disetiap nafas dan hidayah disetiap masalah, sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan baik.
2. Kedua orang tua dan keluarga, yang selalu menjadi alasan untuk berusaha dan berjuang.
3. Bapak Prof. Dr. Agus Setyo Budi M.Sc., selaku Rektor Universitas Budi Luhur.
4. Bapak Dr. Ir. Achmad Solichin, S.Kom., M.T.I., selaku Dekan Fakultas Teknologi Informasi.
5. Bapak Bima Dr. Indra, S.Kom, M.T.I., selaku Ketua Program Studi Teknik Informatika.
6. Ibu Reva Ragam Santika, S.Kom., M.Kom., M.M., selaku Dosen Pembimbing Tugas Akhir yang telah banyak membantu, membimbing, dan mendukung dalam penulisan selama proses penyusunan Tugas Akhir.
7. Bapak Dr. Utomo Budiyanto, M.Kom, M.Sc., selaku Dosen Penasehat Akademik
8. Bapak Jahidin, selaku pemilik Rumah Makan Mitra Minang yang telah memberikan kesempatan untuk melakukan penelitian kali ini
9. Semua pihak yang telah membantu dan tidak dapat saya sebutkan satu persatu. Semoga atas segala kebaikan dan bimbingannya mendapatkan berkah dan rahmat dari Allah SWT.

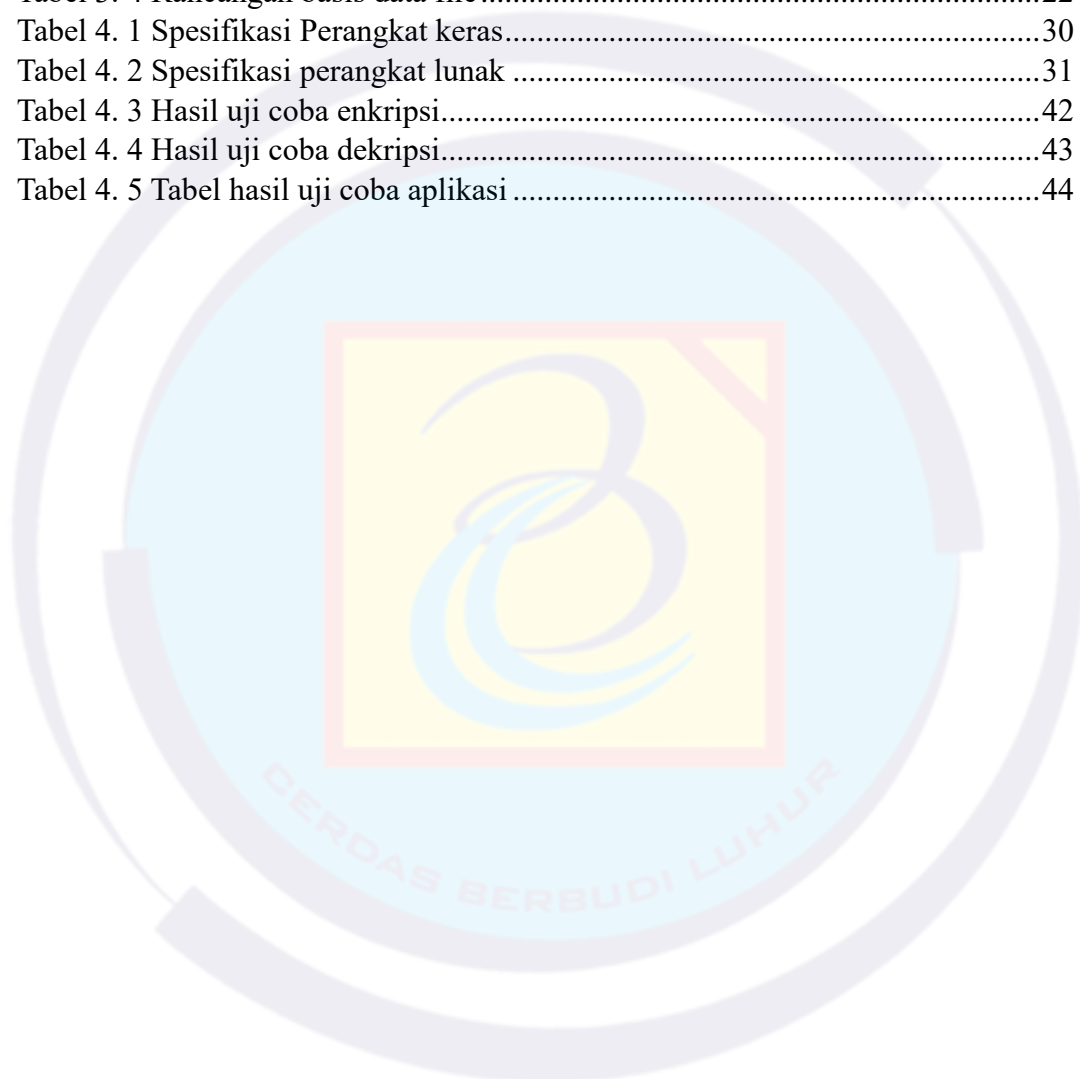
Akhir kata penulis sangat menyadari bahwa dalam pengerjaanya dan penulisannya tugas akhir ini masih jauh dari kata sempurna, karena dari keterbatasan ilmu yang penulis miliki. Sebab karena itu kritik dan saran yang membangun dari berbagai pihak sangat penulis harapkan demi perbaikan kedepannya. Semoga laporan ini bermanfaat bagi pembaca, terutama mahasiswa Universitas Budi Luhur.

Jakarta, 29 Juli 2024

Penulis

## DAFTAR TABEL

Tabel 2. 1 Jumlah proses yang terdiri dari bit blok dan kunci .....	7
Tabel 2. 2 Studi Literatur .....	12
Tabel 3. 1 Perbedaan dari Penelitian Sebelumnya .....	18
Tabel 3. 2 Rancangan Pengujian .....	21
Tabel 3. 3 Rancangan basis data users .....	22
Tabel 3. 4 Rancangan basis data file .....	22
Tabel 4. 1 Spesifikasi Perangkat keras .....	30
Tabel 4. 2 Spesifikasi perangkat lunak .....	31
Tabel 4. 3 Hasil uji coba enkripsi .....	42
Tabel 4. 4 Hasil uji coba dekripsi .....	43
Tabel 4. 5 Tabel hasil uji coba aplikasi .....	44



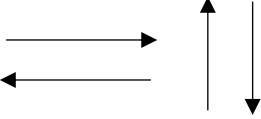
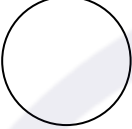
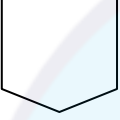


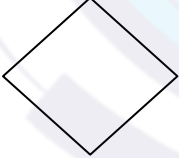


## DAFTAR GAMBAR

Gambar 2. 1 Kunci dengan skema enkripsi dan deskripsi .....	5
Gambar 2. 2 Proses <i>SubByte</i> dengan <i>S-Box</i> .....	8
Gambar 2. 3 Proses <i>Shiftrows</i> .....	9
Gambar 2. 4 Proses <i>Mixcolumns</i> .....	9
Gambar 2. 5 Proses <i>AddRoundKey</i> .....	10
Gambar 2. 6 Diagram Alur Enkripsi AES .....	11
Gambar 2. 7 Diagram Alur Dekripsi AES .....	11
Gambar 3. 1 Rancangan menu .....	23
Gambar 3. 2 Tampilan rancangan layar pada menu <i>login admin</i> .....	24
Gambar 3. 3 Tampilan rancangan layar pada menu <i>login</i> pegawai atau kasir .....	24
Gambar 3. 4 Tampilan rancangan layar pada menu awal <i>admin</i> .....	25
Gambar 3. 5 Tampilan rancangan layar pada menu awal pegawai atau kasir .....	26
Gambar 3. 6 Tampilan rancangan layar pada menu enkripsi <i>admin</i> .....	27
Gambar 3. 7 Tampilan rancangan layar pada menu enkripsi pegawai atau kasir .....	27
Gambar 3. 8 Tampilan rancangan layar pada menu dekripsi <i>admin</i> .....	28
Gambar 3. 9 Tampilan rancangan layar pada submenu dekripsi <i>admin</i> .....	28
Gambar 3. 10 Tampilan rancangan layar pada menu pegawai pengguna <i>admin</i> .....	29
Gambar 3. 11 Tampilan rancangan layar pada submenu pegawai <i>admin</i> .....	29
Gambar 4. 1 <i>Deployment Diagram</i> .....	31
Gambar 4. 2 <i>Flowchart</i> tahapan menu <i>login</i> .....	32
Gambar 4. 3 <i>Flowchart</i> tahapan level status pengguna .....	33
Gambar 4. 4 <i>Flowchart</i> tahapan level pengguna <i>admin</i> .....	34
Gambar 4. 5 <i>Flowchart</i> tahapan level pengguna pegawai .....	34
Gambar 4. 6 <i>Flowchart</i> tahapan menu <i>upload file</i> untuk enkripsi .....	35
Gambar 4. 7 <i>Flowchart</i> tahapan proses pada enkripsi .....	36
Gambar 4. 8 <i>Flowchart</i> tahapan proses pada menu dekripsi .....	37
Gambar 4. 9 <i>Flowchart</i> tahapan proses pada dekripsi .....	38
Gambar 4. 10 <i>Flowchart</i> tahapan pada menu pegawai .....	39
Gambar 4. 11 <i>program</i> proses enkripsi .....	40
Gambar 4. 12 <i>program</i> proses dekripsi .....	40
Gambar 4. 13 Contoh <i>file</i> pdf asli nota penjualan sebelum dienkripsi .....	41
Gambar 4. 14 Contoh <i>file</i> pdf asli nota penjualan setelah dienkripsi .....	42
Gambar 4. 15 Menu halaman <i>login admin</i> dan pegawai .....	45
Gambar 4. 16 Menu halaman awal <i>admin</i> .....	46
Gambar 4. 17 Menu halaman awal pegawai atau kasir .....	46
Gambar 4. 18 Menu halaman enkripsi <i>admin</i> dan pegawai .....	47
Gambar 4. 19 Menu halaman dekripsi <i>file admin</i> .....	48
Gambar 4. 20 Menu halaman proses dekripsi <i>file admin</i> .....	48
Gambar 4. 21 Menu halaman tambah pegawai <i>admin</i> .....	49
Gambar 4. 22 Menu halaman proses tambah pegawai .....	49



## DAFTAR SIMBOL

	<p><b>Flow</b></p> <p>Simbol yang digunakan untuk menggabungkan antara simbol yang satu dengan simbol yang lain. Simbol ini disebut juga dengan <i>Connecting Line</i>.</p>
	<p><b>On-Page Reference</b></p> <p>Simbol untuk keluar – masuk atau penyambungan proses dalam lembar kerja yang sama.</p>
	<p><b>Off-Page Reference</b></p> <p>Simbol untuk keluar – masuk atau penyambungan proses dalam lembar kerja yang berbeda.</p>
	<p><b>Terminator</b></p> <p>Simbol yang menyatakan awal atau akhir suatu program.</p>
	<p><b>Process</b></p> <p>Simbol yang menyatakan suatu proses yang dilakukan komputer.</p>
	<p><b>Decision</b></p> <p>Simbol yang menunjukan kondisi tertentu yang akan menghasilkan dua kemungkinan jawaban, yaitu ya dan tidak.</p>

## DAFTAR ISI

LEMBAR PENGESAHAN .....	iii
ABSTRAK .....	iv
SURAT PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN PUBLIKASI .....	v
KATA PENGANTAR.....	vi
DAFTAR TABEL .....	vii
DAFTAR GAMBAR.....	viii
DAFTAR SIMBOL .....	ix
DAFTAR ISI.....	x
BAB I.....	1
PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan .....	2
1.5 Manfaat .....	2
1.6 Sistematika Penulisan .....	3
BAB II.....	4
LANDASAN TEORI .....	4
2.1 Keamanan Informasi Data .....	4
2.2 Kriptografi.....	4
2.3 Sejarah Kriptografi.....	6
2.3.1 Jenis kriptografi .....	6
2.4 Tujuan Kriptografi.....	6
2.5 <i>Advanced Encryption Standard (AES)</i> .....	7
2.5.1 SubBytes .....	8
2.5.2 ShiftRows.....	8
2.5.3 MixColumns .....	9
2.5.4 AddRoundKey .....	10
2.6 Enkripsi AES .....	10

2.7	Dekripsi AES.....	10
2.8	Penelitian Sebelumnya.....	12
<b>BAB III.....</b>		<b>18</b>
<b>METODOLOGI PENELITIAN.....</b>		<b>18</b>
3.1	Data Penelitian .....	18
3.2	Metode Pembandingan .....	18
3.3	Penerapan Metode yang digunakan .....	20
3.4	Rancangan Pengujian .....	20
3.5	Rancangan Basis Data .....	22
3.6	Rancangan Menu .....	23
3.7	Rancangan Layar.....	23
3.7.1	Rancangan Layar Pada Menu <i>Login</i> .....	23
3.7.2	Rancangan Layar Pada Menu Awal .....	25
3.7.3	Rancangan Layar Pada Menu Unggah <i>File</i> .....	26
3.7.4	Rancangan Layar Pada Menu Pegawai Pengguna <i>Admin</i> .....	29
<b>BAB IV.....</b>		<b>30</b>
<b>HASIL DAN PEMBAHASAN.....</b>		<b>30</b>
4.1	Lingkungan Percobaan.....	30
4.1.1	Spesifikasi Perangkat Keras.....	30
4.1.2	Spesifikasi Perangkat Lunak.....	30
4.1.3	<i>Deployment Diagram</i> .....	31
4.2	Implementasi Metode.....	31
4.3	Flowchart .....	32
4.3.1	Flowchart Menu Login .....	32
4.3.2	Flowchart Menu Level Status Pengguna .....	33
4.3.3	Flowchart Pada Proses Enkripsi .....	35
4.3.4	Flowchart Pada Proses Dekripsi Pengguna Admin.....	36
4.3.5	Flowchart Pada Menu Pegawai.....	38
4.4	Algoritma .....	39
4.5	Pengujian .....	41
4.5.1	Pengujian Enkripsi.....	41
4.5.2	Kesimpulan Hasil Uji Coba Enkripsi dan Dekripsi .....	42

<b>4.6</b>	<b>Tampilan Layar Aplikasi .....</b>	<b>45</b>
4.6.1	Menu Halaman <i>Login Admin</i> dan Pegawai.....	45
4.6.2	Menu Halaman Utama <i>Admin</i> dan Pegawai .....	46
4.6.3	Menu Halaman Unggah <i>File Admin</i> dan Kasir.....	47
4.6.4	Menu Halaman Pegawai Pada <i>Admin</i> .....	49
<b>4.7</b>	<b>Evaluasi Program.....</b>	<b>50</b>
<b>BAB V</b>	<b>.....</b>	<b>51</b>
<b>PENUTUP</b>	<b>.....</b>	<b>51</b>
<b>5.1</b>	<b>Kesimpulan .....</b>	<b>51</b>
<b>5.2</b>	<b>Saran.....</b>	<b>51</b>
<b>DAFTAR PUSTAKA</b>	<b>.....</b>	<b>52</b>
<b>LAMPIRAN</b>	<b>.....</b>	<b>54</b>
<b>Lampiran 1 : SURAT KETERANGAN RISET</b>	<b>.....</b>	<b>54</b>
<b>Lampiran 2 : Hasil Cek <i>Similarity</i></b>	<b>.....</b>	<b>55</b>

## BAB I PENDAHULUAN

### 1.1 Latar Belakang

Dengan berkembangnya sebuah teknologi yang semakin cepat teknologi informasi memiliki efek negatif dan positif. Salah satu konsekuensi negatif dari kemajuan teknologi adalah adanya penyalahgunaan data. Maka keamanan dan kerahasiaan data perusahaan sangatlah penting pada masa kini. Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data. Data dapat berupa dokumen digital seperti *word*, PDF, dan *excel*, bahkan nota penjualan maupun pembelian. Dan maka semisal apabila ada dari pihak yang tidak berkepentingan mencoba mengakses atau mengubah data tersebut, maka sangat dikhawatirkan akan terjadinya hal yang tidak diinginkan. Oleh sebab itu dibutuhkanlah suatu aplikasi yang bisa dapat menjaga keamanan suatu data bahkan nota suatu penjualan dan pembelian (Pramusinto, Wizaksono & Saputro, 2019).

Rumah Makan Mitra Minang merupakan suatu usaha UMKM (Usaha Mikro Kecil dan Menengah) yang bergerak dalam usah pada kuliner yang berpusat dikota Jakarta. Adanya dampak negatif dari penyalahgunaan data nota penjualan dan pembelian hasil transaksi pada pelanggan oleh para oknum yang tidak bertanggung jawab. Maka dibuatlah sistem keamanan kriptografi AES (*Advanced Encryption Standard*) untuk menjaga kerahasiaan dan keamanan sebuah data atau nota.

Kriptografi adalah seni dan ilmu untuk memastikan pesan aman. Menurut buku-buku yang diterbitkan sebelum tahun 1980-an, kriptografi adalah seni dan ilmu untuk menjaga kerahasiaan pesan dengan menyandikannya ke dalam bentuk yang tidak dapat dibaca dan tidak dapat ditafsirkan lagi. Kriptografi juga didefinisikan sebagai bidang yang mempelajari metode matematika yang berkaitan dengan elemen keamanan informasi seperti kerahasiaan, integritas, dan otentikasi (Munir, 2006).

Pada konsep ini metode penerapan enkripsi dan dekripsi menjadi sebuah solusi yang amat penting untuk melindungi data nota penjualan dan pembelian Rumah Makan Mitra Minang. Dengan sebuah metode teknik enkripsi yang digunakan adalah AES (*Advanced Encryption Standard*) dengan kunci bit 128. Pada AES-128 memiliki kelebihan keamanan data dan kemampuan untuk digunakan pada berbagai jenis perangkat keras dan lunak. Dengan penerapan menggunakan AES-128 ini maka Rumah Makan Mitra Minang dapat meningkatkan keamanan dan mencegah adanya penyalahgunaan dari pihak yang tidak bertanggung jawab.

Maka dalam penelitian ini berguna untuk membangun sebuah sistem keamanan AES berbasis web pada data dengan AES-128 dan diaplikasikan dengan enkripsi *file* dan dekripsi *file* melalui sebuah web. Dalam penelitian ini sangat diharapkan dapat memberikan sebuah partisipasi yang sangat berarti dalam peningkatan keamanan serta kerahasiaan data nota informasi penting bagi Rumah Makan Mitra Minang. Penelitian ini juga diharapkan dapat memberikan peran penting serta pada

pengetahuan tentang keamanan dari suatu data di era *modern* yang selalu berkembang ini, serta memberikan rekomendasi praktis untuk para pegiat usaha UMKM lain dalam bidang yang serupa.

### 1.2 Perumusan Masalah

1. Bagaimana cara untuk mengamankan suatu data transaksi ?
2. Bagaimana cara menggunakan *Advanced Encryption Standard* (AES) ?
3. Bagaimana cara membuat aplikasi keamanan data berbasis web menggunakan algoritma *Advanced Encryption Standard* (AES) ?

### 1.3 Batasan Masalah

Berdasarkan pemaparan identifikasi masalah penelitian ini menetapkan beberapa batasan masalah sebagai berikut :

1. Dalam penelitian ini membatasi panjang kunci AES hanya sampai 16 karakter atau 128 bit.
2. Ukuran *file* enkripsi tidak bisa begitu besar hanya sekitar 2 MB.
3. Menggunakan bahasa pemrograman PHP, yang dapat mengenkripsi dan mendekripsi *file* dalam format docx, pdf, xlsx, pptx, dan jpg.
4. Dalam penelitian ini data yang digunakan adalah data nota penjualan dan pembelian dari Rumah Makan Mitra Minang.

### 1.4 Tujuan

Adapun tujuan penelitian ini sebagai berikut :

1. Untuk mendapatkan pemahaman tentang bagaimana membuat sistem yang dapat menjaga keamanan dari suatu data.
2. Mengetahui cara menggunakan *Advanced Encryption Standard* (AES).
3. Membuat aplikasi keamanan data dengan enkripsi dan dekripsi berbasis web.

### 1.5 Manfaat

Adapun manfaat penelitian ini sebagai berikut :

1. Dapat diharapkan menjadi sumber literasi untuk meningkatkan pengetahuan peneliti.
2. Membantu meningkatkan perlindungan data terhadap pihak yang tidak bertanggung jawab.
3. Memberikan rekomendasi kepada para pegiat usaha kecil atau besar untuk menggunakan sistem keamanan yang serupa.



## **1.6 Sistematika Penulisan**

Untuk mempermudah pencarian informasi, penelitian ini akan dibagi menjadi 5 bab. Penulisannya akan disusun sebagai berikut :

### **BAB I : PENDAHULUAN**

Pada bab ini penulis menjelaskan latar belakang penelitian, identifikasi masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

### **BAB II : LANDASAN TEORI**

Beberapa subbab, termasuk pencapaian terdahulu, dan tinjauan teoritis akan mencakup berbagai teori yang akan membantu penulis menyusun laporan dan melakukan penelitian tentang kriptografi AES-128

### **BAB III : METODOLOGI PENELITIAN**

Pada bab ini penulis membahas beberapa tahapan metodologi yang digunakan untuk menyelesaikan masalah dan solusi yang dibahas dalam tugas akhir termasuk tahapan penelitian, metode pengumpulan data, tahapan pengolahan data perbandingan penelitian sebelumnya. Serta analisa program aplikasi, rancangan layar aplikasi.

### **BAB IV : HASIL DAN PEMBAHASAN**

Penulis membahas spesifikasi hardware dan software aplikasi, implementasinya, dan cara pengoperasiannya, serta evaluasinya, yang mencakup kelebihan dan kekurangan aplikasi.

### **BAB V : PENUTUP**

Pada bab ini menyampaikan kesimpulan dan saran dari diskusi topik tugas akhir penelitian dan memberikan rekomendasi untuk meningkatkan topik tersebut di masa depan.

## BAB II

### LANDASAN TEORI

#### 2.1 Keamanan Informasi Data

Keamanan data merupakan hal, yang mencakup perlindungan data digital maupun *non* digital dari akses, penggunaan, atau pengungkapan yang tidak sah sesuai dengan strategi risiko organisasi. Ini juga mencakup perlindungan data dari gangguan, modifikasi, atau penghancuran. Data sangatlah penting bagi kehidupan setiap organisasi dan juga sangat penting bagi keberhasilan suatu perusahaan, jadi penting bagi organisasi dari semua ukuran untuk melindunginya. Keamanan data sangat penting untuk menjaga data organisasi tetap rahasia, jujur, dan tersedia. Dengan menerapkan langkah-langkah keamanan data yang kuat, perusahaan dapat memenuhi persyaratan kepatuhan, menjaga kepercayaan pelanggan, dan melindungi aset berharga mereka (Oktavani et al., 2023).

Aspek *confidently* dimaksudkan untuk mencegah data komputer jatuh ke tangan yang tidak berhak. Untuk meningkatkan keamanan komputer, *password* digunakan untuk mencegah orang yang tidak berhak mengakses data pribadi (rahasia), mencegah data dimanipulasi atau dirusak (integritas), dan memberikan autentikasi kepada pihak yang berhak untuk mengakses data tersebut (Pratiwi, 2016).

Ada dua cara untuk melindungi data, kriptografi dengan algoritma *Advanced Encryption Standard* (AES) dan steganografi dengan *Command/DOS* (Pabokory et al., 2015)

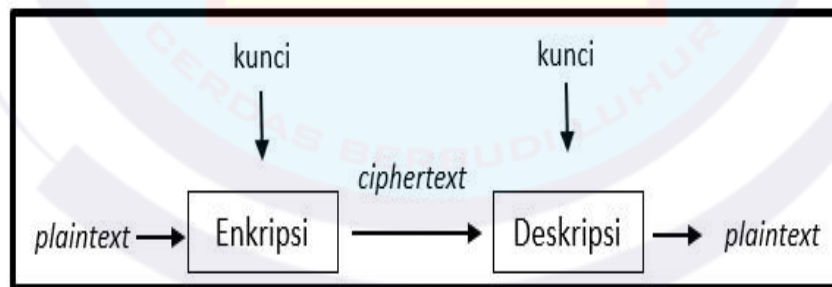
#### 2.2 Kriptografi

Kriptografi adalah proses menyembunyikan atau mengkodekan data sehingga hanya individu yang dimaksud dapat membacanya. Selama ribuan tahun, seni kriptografi telah digunakan untuk mengkodekan pesan. Ini masih digunakan dalam kata sandi komputer, kartu bank, dan *e-commerce*. Alat kriptografi kontemporer termasuk algoritma dan sandi yang memungkinkan enkripsi dan dekripsi data, seperti kunci enkripsi 128-bit dan 256-bit. Sandi kontemporer, seperti Standar Enkripsi Tinggi (AES), dianggap tidak dapat dipecahkan. Kriptografi, juga dikenal sebagai kriptologi, adalah teknik keamanan siber yang menggunakan kode informasi untuk memastikan hanya orang yang menerima pesan yang dapat membaca dan memprosesnya. Teknik ini menggabungkan berbagai disiplin ilmu seperti ilmu komputer, teknik, dan matematika untuk membuat kode kompleks yang menyembunyikan makna sebenarnya dari sebuah pesan (Lyman, C. 2022).

Didalam kriptografi sering menggunakan berbagai istilah atau *terminology*. Ada beberapa istilah yang harus dipahami, yaitu :

1. *Ciphertexts*, *plaintexts*, 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* (Lyman, C. 2022).
2. Pengirim atau penerima adalah komunikasi yang melibatkan pertukaran pesan dengan dua atau lebih. Pengirim (*sender*) adalah orang yang mengirim pesan kepada penerima lainnya. Penerima (*receiver*) adalah orang yang menerima pesan (Pabokory, et al., 2015).
3. Enkripsi dan dekripsi adalah proses mengubah data atau informasi yang akan dikirim menjadi bentuk yang hampir tidak dikenal sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi, yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awalnya (Muharram, et al., 2018).
4. *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* (Lyman, C. 2022).

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 2.1



Gambar 2. 1 Kunci dengan skema enkripsi dan deskripsi

## 2.3 Sejarah Kriptografi

Kriptografi memiliki sejarah yang luas dan luar biasa. Penulisan rahasia ini digunakan oleh Mesir pada tahun 3000 tahun SM. Mereka menyembunyikan tulisan orang asing dengan hieroglyphics. "*Hieroglyphics*" berasal dari kata Yunani "*hieroglyphica*", yang berarti "ukiran rahasia". Hieroglyphs berevolusi menjadi hieratic, yang berarti skrip yang distylized yang lebih mudah digunakan. Sekitar tahun 400 tahun SM, bangsa *Spartan* menggunakan kriptografi militer dalam bentuk sepotong papyrus atau perkamen yang dibungkus dengan batang kayu. *Scytale* adalah nama pembuat sistem ini (Amalya, 2023).

### 2.3.1 Jenis kriptografi

#### a. *Hash Function*

*Hash function* digunakan untuk meringkas data dan memberikan penjelasan yang telah diringkaskan. *Cryptography* jenis ini menggunakan persamaan matematika algoritma mengambil nilai numerik dan kemudian diringkaskan oleh *hash system* (Adani, 2021).

#### b. *Public Key Cryptography*

*Public key cryptography* adalah ide yang revolusioner untuk melindungi data selama 300 hingga 400 tahun terakhir. Istilah "kunci publik" mengacu pada dua kunci yang saling berhubungan, kunci publik dan privat (Adani, 2021).

*Public key cryptography* dianggap lebih aman jika dibandingkan dengan kriptografi kunci simetris. Metode RSA adalah yang paling umum untuk jenis kriptografi ini, dan teknik lain seperti DSA, PKC, dan teknik kurva elips (Adani, 2021).

#### c. *Symmetric Key Cryptography*

Jenis *symmetric key cryptography* yang dikenal sebagai kunci rahasia memungkinkan penerima dan pengirim data menggunakan satu kunci untuk mengenkripsi data. AES adalah sistem kriptografi canggih yang digunakan. Metode kunci simetri dianggap lebih efektif daripada metode lain (Adani, 2021).

## 2.4 Tujuan Kriptografi

Dari paparan yang disampaikan diatas dirangkumkan bahwa, kriptografi memberi sebuah layanan keamanan. Berikut tujuan dari kriptografi :

### 1. Kerahasiaan (*confidentiality*)

Adalah layanan yang dimaksudkan untuk memastikan bahwa pesan tidak dapat dibaca oleh pihak yang tidak berhak. Dengan aspek kerahasiaan ini akan didukung dengan memanfaatkan algoritma dari kriptografi yaitu, algoritma enkripsi dan

dekripsi baik itu dengan simetri ataupun asimetri. Dalam aspek kali ini sangat terkait dengan adanya kunci sehingga kunci tidak disalahgunakan dengan pihak yang tidak bertanggung jawab (kurniati, 2019).

## 2. Integritas data (data integrity)

Adalah layanan dengan aspek integritas yang didukung dengan memanfaatkan algoritma *hash*. Fungsi *hash* memastikan bahwa pesan yang dikirim asli dan tidak diubah selama pengiriman (kurniati, 2019).

## 3. Otentikasi (authentication)

Adalah layanan yang mempunyai aspek keamanan informasi yang dapat didukung dengan melalui mekanisme tanda tangan yang berupa digital. identifikasi yang mengidentifikasi kebenaran pihak yang berkomunikasi (*user authentication*) (kurniati, 2019).

### 2.5 Advanced Encryption Standard (AES)

*Advanced Encryption Standard* (AES) adalah algoritma kriptografi yang memiliki kemampuan untuk digunakan dalam keamanan data. Algoritma AES adalah blok *chipertext* simetrik yang memiliki kemampuan untuk mengenkripsi (*encipher*) dan dekripsi (*decipher*) data. Enkripsi mengubah data dan membuatnya tidak dapat dibaca ini disebut *ciphertext*. Dekripsi, sebaliknya mengubah data *ciphertext* ke format aslinya yang dikenal sebagai *plaintext*. Algoritma AES mengenkrip dan dekrip data pada blok 128 bits dengan kunci kriptografi 128, 192, dan 256 bits. Memilih ukuran blok data dan kunci akan menentukan berapa banyak proses yang perlu dilakukan untuk enkripsi dan dekripsi (Kridalaksana, 2015).

Pada perbandingan yang akan dilakukan untuk masing-masing masukan bisa dilihat pada Tabel 2.1.

Tabel 2. 1 Jumlah proses yang terdiri 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

Data masukan dan blok kunci dioperasikan dalam *array*. Sebelum menghasilkan keluaran *ciphertext*, setiap anggota *array* diberi nama *state*. *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns* adalah empat langkah yang akan dilakukan oleh setiap *state*. Ketiga tahap lainnya akan diulang pada setiap proses kecuali tahap *MixColumns* namun, tahap *MixColumns* tidak akan dilakukan pada tahap terakhir.



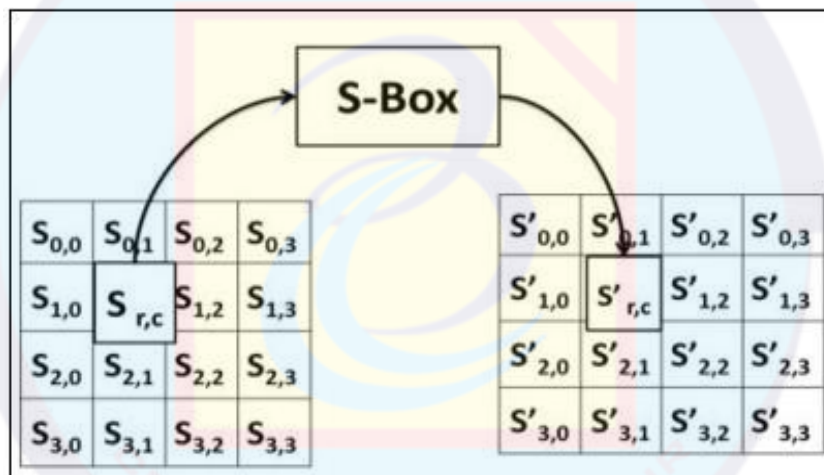
AES mempunyai 4 jenis transformasi yang digunakan, yaitu :

1. *SubBytes* berfungsi sebagai transformasi substitusi.
2. *ShiftRows* berfungsi sebagai transformasi permutasi.
3. *MixColumns* berfungsi sebagai transformasi pengacakan
4. *AddRoundKey* berfungsi sebagai transformasi penambahan kunci.

### 2.5.1 *SubBytes*

*SubBytes* adalah transformasi *byte* di mana setiap elemen pada state akan dipetakan dalam tabel substitusi, juga dikenal sebagai S-Box. Pensubstitusian dilakukan dengan cara berikut, jika setiap byte pada array state  $S[r,c]=xy$ ,  $xy$  adalah digit heksadesimal dari nilai  $S[r,c]$ , maka nilai substitusi dinyatakan dengan  $S'[r,c]$ , adalah elemen didalam S-Box yang terdiri atas baris  $x$  dan kolom  $y$  (Digilib Unila, n.d.).

Proses *SubBytes* dapat dilihat pada Gambar 2.2.



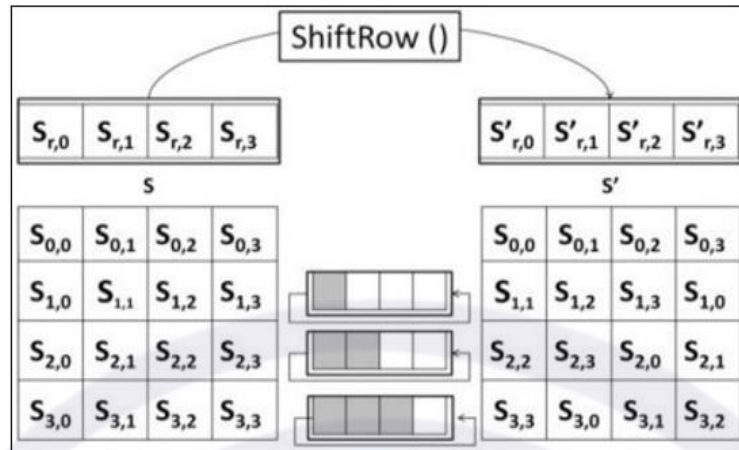
Gambar 2. 2 Proses *SubByte* dengan S-Box

### 2.5.2 *ShiftRows*

Seperti namanya, *Shiftrows* adalah proses yang mengubah atau mengubah setiap elemen *blok* atau tabel yang berjalan di setiap barisnya. Misalnya, baris pertama tidak melakukan pergeseran, baris kedua melakukan pergeseran satu *byte*, baris ketiga melakukan pergeseran dua *byte*, dan baris keempat melakukan pergeseran tiga *byte* (Universitas Esa Unggul, n.d.).



Proses *ShiftRows* dapat dilihat pada Gambar 2.3.

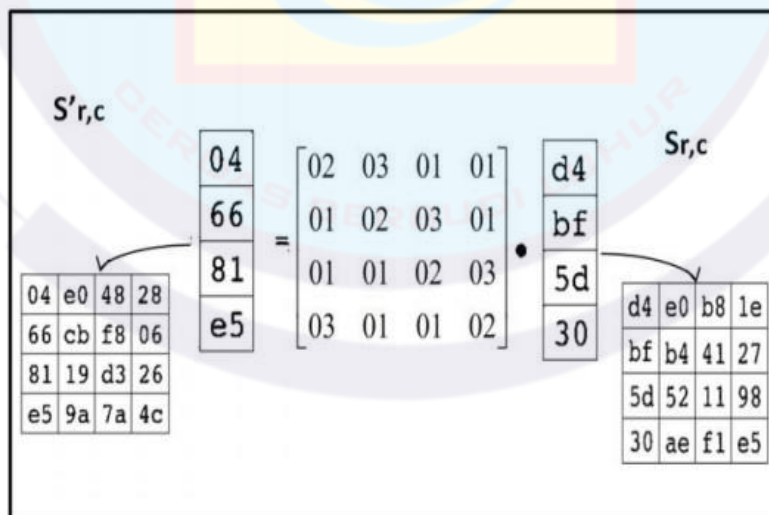


Gambar 2. 3 Proses *Shiftrows*

### 2.5.3 *MixColumns*

Mengalikan semua elemen *block chiper* dengan matriks yang ditunjukkan pada proses sebelumnya adalah apa yang terjadi saat *MixColumns* terjadi. Tabel sudah diatur dan siap digunakan. Pengalian dilakukan dengan cara yang sama seperti dalam perkalian matriks, menggunakan dot dan kemudian lalu menggabungkan keduanya kedalam sebuah *block* pada *cipher* baru *byte* (Universitas Esa Unggul, n.d.).

Proses *Mixcolumns* dapat dilihat pada Gambar 2.4.

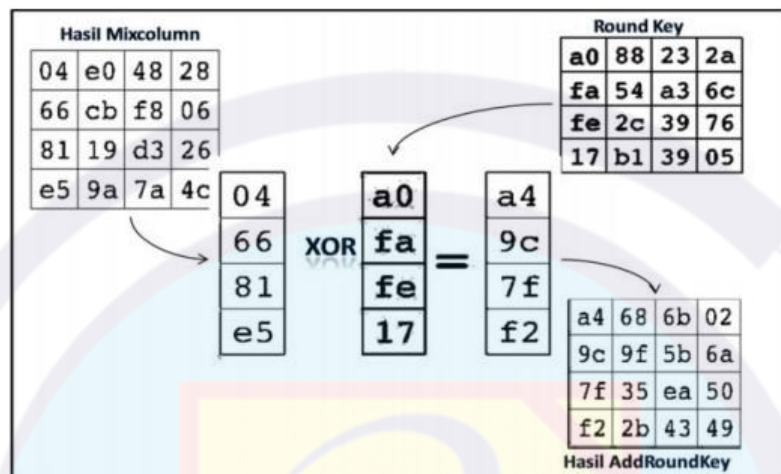


Gambar 2. 4 Proses *Mixcolumns*

#### 2.5.4 AddRoundKey

Dalam proses *AddRoundKey* ini, sebuah operasi XOR dilakukan terhadap sebuah *Key Round* dalam array state, dan hasilnya disimpan dalam array state. *byte* (Universitas Esa Unggul, n.d.).

Proses *AddRoundKey* dapat dilihat pada Gambar 2.5.



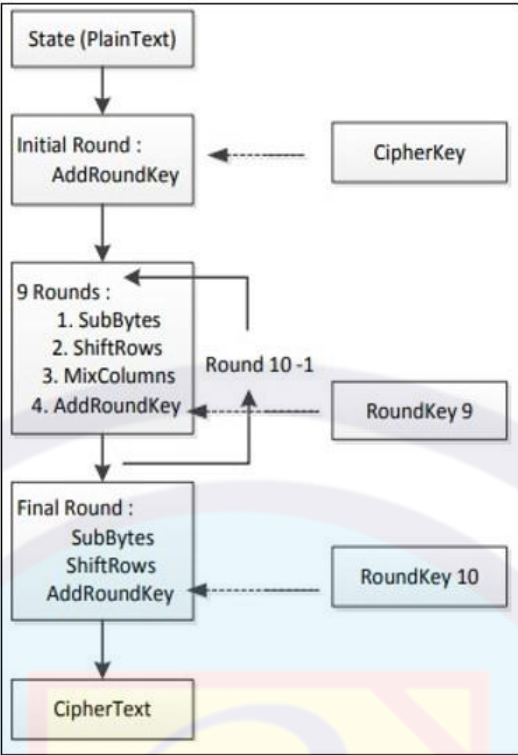
Gambar 2. 5 Proses *AddRoundKey*

#### 2.6 Enkripsi AES

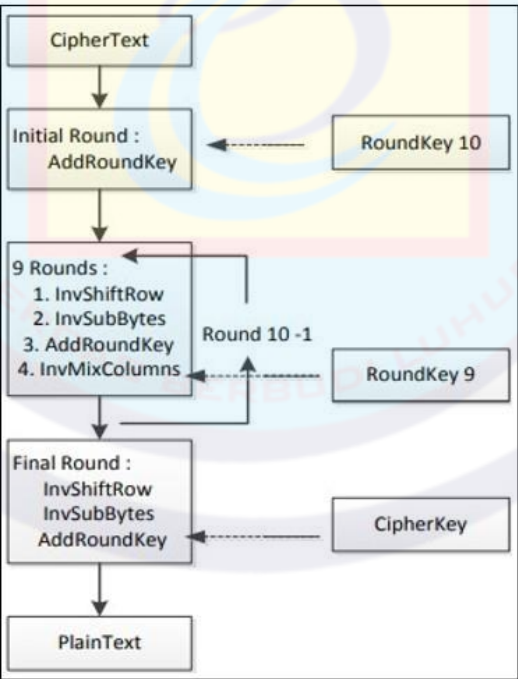
Pada dalam algoritma AES, proses enkripsi terdiri dari dalam 4 jenis transformasi *byte* yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. *Input* yang dikopikan pada kedalam *state* akan diubah menjadi ke *byte AddRoundKey* pada awal proses enkripsi. Dan selanjutnya *state* akan mengubah *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* sebanyak *Nr*. Dalam algoritma AES, prosedur ini dikenal sebagai round function. Dibandingkan dengan ronde sebelumnya, pada ronde terakhir tidak mengalami yang namanya transformasi *MixColumns* (Astuti, 2015). Diagram alur enkripsi AES bisa dilihat pada Gambar 2.6.

#### 2.7 Dekripsi AES

Untuk membuat *inverse cipher* yang mudah dipahami untuk algoritma AES, transformasi *cipher* dapat dibalik dan digunakan dalam arah yang berlawanan. *InvShiftRows*, *InvSubBytes*, *InvMixColumns* dan *Addroundkey* adalah transformasi *byte* yang digunakan untuk *invers cipher* (Astuti, 2015). Diagram alur dekripsi AES bisa dilihat pada Gambar 2.7.



Gambar 2. 6 Diagram Alur Enkripsi AES



Gambar 2. 7 Diagram Alur Dekripsi AES

## 2.8 Penelitian Sebelumnya

Penelitian ini menggunakan berbagai referensi dari penelitian-penelitian sebelumnya sebagai literatur. Sumber referensi untuk tugas akhir kuliah ini berasal dari berbagai jurnal tugas akhir dan jurnal yang terkait dengan topik yang dibahas. Referensi untuk penelitian saat ini bisa dilihat dalam Table 2.1.

Tabel 2. 2 Studi Literatur

No	Penulis	Judul	Tahun	Metode	Hasil
1	Fresly Nandar Pabokory, Indah Fitri Astuti dan Awang Harsa Kridalaksana	Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File dan File Dokumen Menggunakan Algoritma <i>Advanced Encryption Standard</i>	2015	<i>Advanced Encryption Standard</i> (AES)	Hasil dari penelitian yaitu pengguna dapat mengenkripsi pesan teks kemudian disimpan menjadi sebuah <i>file</i> dokumen dan isi <i>file</i> dokumen tersebut dienkripsi lagi selanjutnya hasil enkripsi isi <i>file</i> dokumen tersebut, <i>file</i> dokumennya dienkripsikan dan selanjutnya dikompresi dan disembunyikan pada sebuah <i>file</i> citra (gambar) agar keamanan data informasi tersebut dapat terjaga keamanannya karena telah dilakukan pengamanan dan penyandian yang berlapislapis.
2	Wahyu Pramusinto, Nugroho Wizaksono dan Ari Saputro	Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman	2019	<i>Advanced Encryption Standard</i> (AES), RC4, dan kompresi Huffman	Aplikasi menggunakan algoritma kompresi Huffman, kemudian dienkripsi menggunakan kriptografi AES 192 dan RC4. Aplikasi ini dibuat berbasis web dengan bahasa pemrograman PHP

No	Penulis	Judul	Tahun	Metode	Hasil
					dan database server MySQL. Dari hasil percobaan didapat kesimpulan bahwa aplikasi ini berhasil mengamankan <i>file</i> sehingga tidak bisa dibaca. Aplikasi ini juga dapat mengembalikan <i>file</i> yang sudah dienkripsi menjadi seperti semula.
3	Faturungi Muharram, Huzain Azis dan Abdul Rachman Manga	Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)	2018	<i>Advanced Encryption Standard (AES)</i>	Dari hasil uji coba pada proses enkripsi dan dekripsi maka dapat disimpulkan bahwa <i>file</i> yang melalui uji coba dekripsi akan berubah bentuk menjadi <i>file</i> yang tak bias dibaca, <i>file</i> dapat kembali kebentuk asli jika melalui proses dekripsi dengan menggunakan kunci yang sama saat enkripsi. Dan waktu proses hasil enkripsi-dekripsi data dapat dipengaruhi oleh besar ukuran data yang akan di uji.
4	Muhammad Arif Hidayah, Nurcahyo Budi Nugoho dan Moch. Iswan Perangin-Angin	Penerapan Kriptografi Menggunakan Algoritma AES untuk Keamanan Data Penjualan Pada PT.Mestika Sakti	2020	<i>Advanced Encryption Standard (AES)</i>	<i>Advanced Encryption Standard (AES)</i> digunakan sebagai sistem dalam pengamanan data yang merupakan algoritma yang cukup rumit dalam perhitungannya untuk mengamankan data yang cukup banyak

No	Penulis	Judul	Tahun	Metode	Hasil
					sehingga dapat mengurangi resiko dalam penyalahgunaan data Penjualan dan dapat mengoptimalkan dalam pengamanan data untuk mengamankan data Penjualan pada PT.Mestika Sakti.
5	Nazmi May Sarah Sianturi, Nurcahyo Budi Nugroho dan Widiarti Rista Maya	Implementasi Kriptografi Untuk Pengamanan Data Aset Perusahaan Pada PT.PLN (Persero) Dengan Menggunakan Metode Algoritma AES 192	2020	AES 192	Algoritma Rivest Shamir Adleman(RSA) dan Caesar Cipher digunakan sebagai sistem dalam pengamanan data yang merupakan algoritma yang cukup rumit dalam perhitungannya untuk mengamankan data yang cukup banyak sehingga dapat mengurangi resiko dalam penyalahgunaan data aset dan dapat mengoptimalkan dalam pengamanan data untuk mengamankan data aset pada PT.PLN.
6	Delisman Hulu, Berto Nadeak dan Soeb Aripin	Implementasi Algoritma AES ( <i>Advanced Encryption Standard</i> ) Untuk Keamanan <i>File</i> Hasil Radiologi di RSU Imelda Medan	2020	<i>Advanced Encryption Standard</i> (AES)	Untuk enkripsi dan deskripsi hasil radiologi dapat diakses dengan webserver atau berbasis web sehingga memudahkan untuk mengaksesnya. Hasil radiologi yang dapat di enkripsi dan deskripsi di penelitian



No	Penulis	Judul	Tahun	Metode	Hasil
					ini hanya berformat jpg dan png, maka diluar dari format tersebut maka otomatis sistem akan menolak proses enkripsi tidak bisa di lanjutkan. Proses kecepatan waktu dalam melakukan proses enkripsi dan deskripsi tergantung ukuran <i>file</i> yang akan <i>upload</i> atau di proses jika semakin kecil <i>file</i> yang akan <i>upload</i> maka waktu proses akan lebih cepat jika <i>file</i> semakin besar maka proses <i>upload file</i> semakin lama.
7	Pratiwi dan Dwi Atmodjo WP	Peningkatan Keamanan Data dengan Metode <i>Cropping Selection Pseudorandom</i>	2016	RC4	Salah satu kelemahan dari <i>Pseudorandom Encryption</i> adalah <i>predictable</i> pada bilangan yang dihasilkan. Ini dapat dipahami karena bilangan random hasil dari <i>Pseudorandom</i> urutan $n+1$ adalah hasil dari bilangan sebelumnya, dengan penambahan <i>crooping</i> dan seleksi bilangan yang dihasilkan menjadi bergantung pada bagian yang diseleksi dan diabaikan, sedemikian sehingga sifat urutan bilangan <i>random</i> berubah, menjadi $n+1$ belum tentu dihasilkan dari bilangan

No	Penulis	Judul	Tahun	Metode	Hasil
					sebelumnya. Sifat inilah yang akan menambah kehandalan enkripsi dengan <i>pseudorandom</i> .
8	Rinmar Siringoringo	Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File	2020	<i>Advanced Encryption Standard (AES)</i>	Hasil penelitian ini diperoleh sistem enkripsi dan dekripsi terhadap plainteks dan kunci simetris ( <i>sessionkey</i> ) dengan kombinasi algoritma Rijndael dan RSA. Hasil enkripsi plainteks pada sistem yang dibangun berupa kode karakter, sedangkan untuk enkripsi <i>sessionkey</i> berupa kode number
9	Dhiya Calista	Sistem Pengamanan Data Menggunakan Kriptografi AES Dan <i>BLOCKCHAIN</i> Berbasis Android	2022	<i>Blockchain dan Advanced Encryption Standard (AES)</i>	Metode <i>Blockchain</i> dapat mendeteksi perubahan data dari penyerang secara cepat dan mudah. Namun, metode <i>Blockchain</i> masih dapat diserang secara pasif, maka dari itu metode AES dipadukan dengan <i>Blockchain</i> sebagai pelengkap yang digunakan untuk mengenkripsi data dari <i>plaintext</i> menjadi <i>ciphertext</i> agar data atau informasi yang

No	Penulis	Judul	Tahun	Metode	Hasil
					ada dapat terhindar dari serangan aktif ataupun pasif
10	Apriliana Tumanggor, Humuntal Rumapea dan Arina Silalahi	Implementasi Algoritma <i>Advance Encryption Standard</i> (AES) Pada Keamanan Dokumen Keuangan (Studi Kasus : CV.Multikreasi Bersama)	2023	<i>Advanced Encyrption Standard</i> (AES)	Dengan adanya aplikasi kriptografi dengan metode AES 128 ini dapat mengamankan <i>file</i> dokumen penting yang ada di CV. Multi Kreasi dan Algoritma AES-128 bit ini berhasil diterapkan pada CV. Multi Kreasi yang dapat menghasilkan beberapa <i>file</i> yang dapat di input pada sistem.

## BAB III

### METODOLOGI PENELITIAN

#### 3.1 Data Penelitian

Untuk penelitian kali ini, menggunakan berkas nota pembelian atau penjualan dari Rumah Makan Mitra Minang. Pada tahap ini, penelitian dilakukan dengan beberapa tahap pengumpulan data seperti melakukan wawancara, studi literatur, dan dokumentasi.

#### 3.2 Metode Pembandingan

Pada Table 3.1 ini dipaparkan perbedaan penelitian sebelumnya dan penelitian saat ini untuk menjadi referensi dalam penelitian kali ini

**Tabel 3. 1 Perbedaan dari Penelitian Sebelumnya**

No	Penulis	Penelitian Sebelumnya	Penelitian Saat Ini
1	Fresly Nandar Pabokory, Indah Fitri Astuti dan Awang Harsa Kridalaksana (2015)	<p>“Implementasi Kriptografi Pengamanan Data Pada Pesan <i>Teks</i>, Isi <i>File</i> dan <i>File</i> Dokumen Menggunakan Algoritma <i>Advanced Encryption Standard</i>”</p> <p>Objek : <i>file</i> dokumen dan pesan <i>teks</i></p> <p>Algoritma : <i>Advanced Encryption Standard</i> (AES)</p> <p>Metodologi : Studi Literatur</p> <p>Hasil : Hasil dari penelitian yaitu pengguna dapat mengenkripsi pesan teks kemudian disimpan menjadi sebuah <i>file</i> dokumen dan isi <i>file</i> dokumen tersebut dienkripsi lagi selanjutnya hasil enkripsi isi <i>file</i> dokumen tersebut, <i>file</i> dokumennya dienkripsikan dan selanjutnya dikompresi</p>	<p>“Penerapan Kriptografi Menggunakan Metode AES Untuk Pengamanan Data Penjualan Rumah Makan Mitra Minang”</p> <p>Objek : Data penjualan dan pembelian</p> <p>Algoritma : <i>Advanced Encryption Standard</i> (AES)</p> <p>Metodologi : Studi literatur, wawancara, dan dokumentasi</p> <p>Hasil : Hasil penelitian menunjukkan bahwa penggunaan AES memberikan lapisan tambahan perlindungan terhadap informasi transaksi, meningkatkan kepercayaan kepada pemilik perusahaan dan mengurangi risiko kebocoran data.</p>

No	Penulis	Penelitian Sebelumnya	Penelitian Saat Ini
		dan disembunyikan pada sebuah <i>file</i> citra (gambar) agar keamanan data informasi tersebut dapat terjaga keamanannya karena telah dilakukan pengamanan dan penyandian yang berlapislapis.	
2	Faturungi Muharram, Huzain Azis dan Abdul Rachman Manga (2018)	<p>“Analisis Algoritma pada Proses Enkripsi dan Dekripsi <i>File</i> Menggunakan <i>Advanced Encryption Standard</i> (AES)”</p> <p>Objek : <i>File</i> gambar</p> <p>Algoritma : <i>Advanced Encryption Standard</i> (AES)</p> <p>Metodologi : Studi Literatur</p> <p>Hasil : Dari hasil uji coba pada proses enkripsi dan dekripsi maka dapat disimpulkan bahwa <i>file</i> yang melalui uji coba dekripsi akan berubah bentuk menjadi <i>file</i> yang tak bias dibaca, <i>file</i> dapat kembali kebentuk asli jika melalui proses dekripsi dengan menggunakan kunci yang sama saat enkripsi. Dan waktu proses hasil enkripsi-dekripsi data dapat dipengaruhi oleh besar ukuran data yang akan di uji.</p>	<p>“Penerapan Kriptografi Menggunakan Metode AES Untuk Pengamanan Data Penjualan Rumah Makan Mitra Minang”</p> <p>Objek : Data penjualan dan pembelian</p> <p>Algoritma : <i>Advanced Encryption Standard</i> (AES)</p> <p>Metodologi : Studi literatur, wawancara, dan dokumentasi</p> <p>Hasil : Hasil penelitian menunjukkan bahwa penggunaan AES memberikan lapisan tambahan perlindungan terhadap informasi transaksi, meningkatkan kepercayaan kepada pemilik perusahaan dan mengurangi risiko kebocoran data.</p>

No	Penulis	Penelitian Sebelumnya	Penelitian Saat Ini
3	Delisman Hulu, Berto Nadeak dan Soeb Aripin (2020)	“Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan <i>File</i> Hasil Radiologi di RSU Imelda Medan” Objek : <i>File</i> radiologi Algoritma : AES 128 Metodologi : Studi literatur, Analisa, dan pengujian Hasil : Untuk enkripsi dan deskripsi hasil radiologi dapat diakses dengan webserver atau berbasis web sehingga memudahkan untuk mengaksesnya. Hasil radiologi yang dapat di enkripsi dan deskripsi di penelitian ini hanya berformat jpg dan png, maka diluar dari format tersebut maka otomatis sistem akan menolak proses enkripsi tidak bisa di lanjutkan.	“Penerapan Kriptografi Menggunakan Metode AES Untuk Pengamanan Data Penjualan Rumah Makan Mitra Minang” Objek : Data penjualan dan pembelian Algoritma : <i>Advanced Encryption Standard</i> (AES) Metodologi : Studi literatur, wawancara, dan dokumentasi Hasil : Hasil penelitian menunjukkan bahwa penggunaan AES memberikan lapisan tambahan perlindungan terhadap informasi transaksi, meningkatkan kepercayaan kepada pemilik perusahaan dan mengurangi risiko kebocoran data.

### 3.3 Penerapan Metode yang digunakan

Pada permasalahan kali ini sangat dibutuhkannya aplikasi yang dapat bisa menjaga kerahasiaan transaksi dari hasil penjualan dan pembelian Rumah Makan Mitra Minang. Pada aplikasi ini nantinya dapat mengubah *file* yang nantinya tidak dapat dilihat dan diubah oleh pihak yang tidak bertanggung jawab. Agar menghilangkan faktor kecurangan yang tidak diinginkan oleh pihak yang tidak bertanggung jawab nantinya *file* tersebut akan dienkripsi atau dirahasiakan, lalu *file* tersebut akan dikembalikan seperti semula atau disebut juga dengan didekripsikan. Aplikasi ini dibuat dengan bahasa pemrograman PHP serta algoritma kriptografi AES-128.

### 3.4 Rancangan Pengujian

Pada aplikasi ini memiliki dua tampilan, satu sebagai *Administrator* (*admin*) dan satu lagi sebagai pegawai. Pada tampilan *Administrator* memiliki tiga



menu utama, yaitu menu halaman utama, menu unggah *file*, dan menu pegawai. menu enkripsi dan dekripsi terletak di menu unggah *file*. Namun pada tampilan pegawai atau kasir hanya akan dapat melihat dua menu utama, yaitu, menu halaman utama dan menu unggah *file*. pada bagian ini menu pada unggah *file* hanya ada enkripsi saja yang ada pada menu unggah *file*.

Pada tampilan pengguna pegawai atau kasir hanya terdapat menu enkripsi saja. Menu enkripsi ini berguna untuk menampilkan *form* untuk mengenkripsi sebuah data, setelah data berhasil terenkripsi akan masuk ke dalam data base yang telah ada, yang mana pegawai hanya berperan sebagai pengirim.

Berbeda dengan pegawai atau kasir, pada tampilan menu unggah *file* pada *admin* menampilkan dua menu, yaitu enkripsi *file* dan dekripsi *file*. Untuk proses enkripsi dan dekripsi, *admin* bisa mengontrol semua proses. Proses ini dapat ditemukan di menu daftar enkripsi dan dekripsi. Rancangan pengujian bisa dilihat dalam Table 3.2.

Tabel 3. 2 Rancangan Pengujian

Kelas Uji	Detail Pengujian	Jenis Pengujian
<i>Login admin</i> atau pegawai	Memverifikasi <i>data login admin</i> dan pegawai dengan memasukkan <i>username</i> dan <i>password</i>	<i>Black box</i>
Pengujian enkripsi <i>file</i>	proses enkripsi mengupload <i>file</i> dengan memilih <i>file</i> yang ingin di upload lalu memasukkan <i>password</i> beserta deskripsi keterangan	<i>Black box</i>
Pengujian dekripsi <i>file</i>	Proses dekripsi dengan memasukkan <i>password</i> yang sama pada <i>file</i> yang dienkripsi	<i>Black box</i>
Pengujian penambahan pegawai	Proses pendaftaran dengan memasukkan <i>username</i> , <i>password</i> , nama, pekerjaan, dan status. Sekaligus proses simpan	<i>Black box</i>

### 3.5 Rancangan Basis Data

Dalam tahap proses ini, dibutuhkan basis data yang berisi semua data untuk menjalankan aplikasi. Rancangan basis data bisa dilihat dalam tabel 3.3 untuk tabel pengguna dan 3.4 untuk tabel *file*.

*Primary Key* : *username*

Isi : data *user*

**Tabel 3. 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*

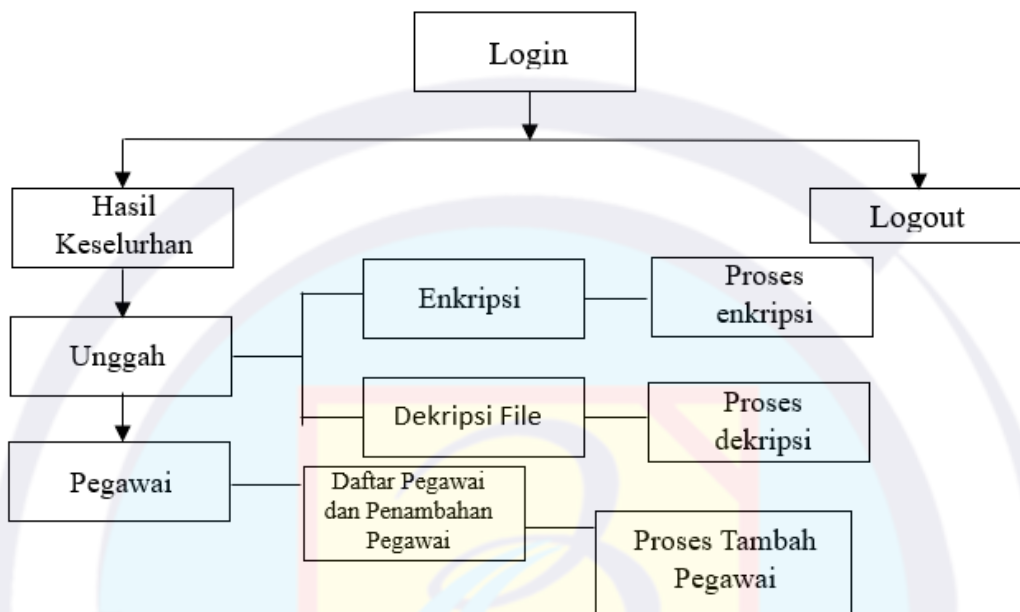
Isi : Data *file*

**Tabel 3. 4 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

### 3.6 Rancangan Menu

Pada tahap rancangan menu ini tahap perancangan menu aplikasi dilakukan untuk membuat aplikasi yang ideal dengan mempertimbangkan faktor masalah dan kebutuhan yang telah disebutkan sebelumnya. Hal ini dilakukan untuk mencapai hasil yang ideal. dan mudah untuk diterapkan. Rancangan menu bisa dilihat pada gambar 3.1.



Gambar 3. 1 Rancangan menu

### 3.7 Rancangan Layar

Dalam proses membuat program, rancangan layar sangat penting karena akan digunakan dalam pembuatan program untuk membantu dalam pembuatan aplikasi yang sedang dirancang. Oleh sebab itu rancangan layar mudah dipahami untuk membuat program yang nyaman untuk digunakan. Rancangan dan desain layar yang disesuaikan untuk kebutuhan para pengguna. Berikut adalah tampilan pada rancangan layar pada aplikasi kriptografi :

#### 3.7.1 Rancangan Layar Pada Menu *Login*

Pada tahap rancangan layar ini adalah untuk menu *login* ke dalam program aplikasi yang mana membutuhkan *username* dan *password* yang sudah terdaftar sebelumnya.

Berikut adalah tampilan layar pada menu *login* untuk *admin* :



The screenshot shows a web browser window with the address bar displaying `http://localhost/ta_kripto/`. The page has a blue background and features the text "Rumah Makan Mitra Minang" at the top. Below this is a "LOGIN" section with a user icon. The login form includes two input fields: "Username" and "Password", both containing placeholder text. At the bottom of the form is a "Login" button with a right-pointing arrow icon.

Gambar 3. 2 Tampilan rancangan layar pada menu *login admin*

Berikut adalah tampilan layar pada menu *login* untuk kasir :



This screenshot is identical to the one above, showing the same login form for "Rumah Makan Mitra Minang". It includes the browser address bar with `http://localhost/ta_kripto/`, the "LOGIN" header, and the "Username", "Password", and "Login" fields and button.

Gambar 3. 3 Tampilan rancangan layar pada menu *login pegawai atau kasir*

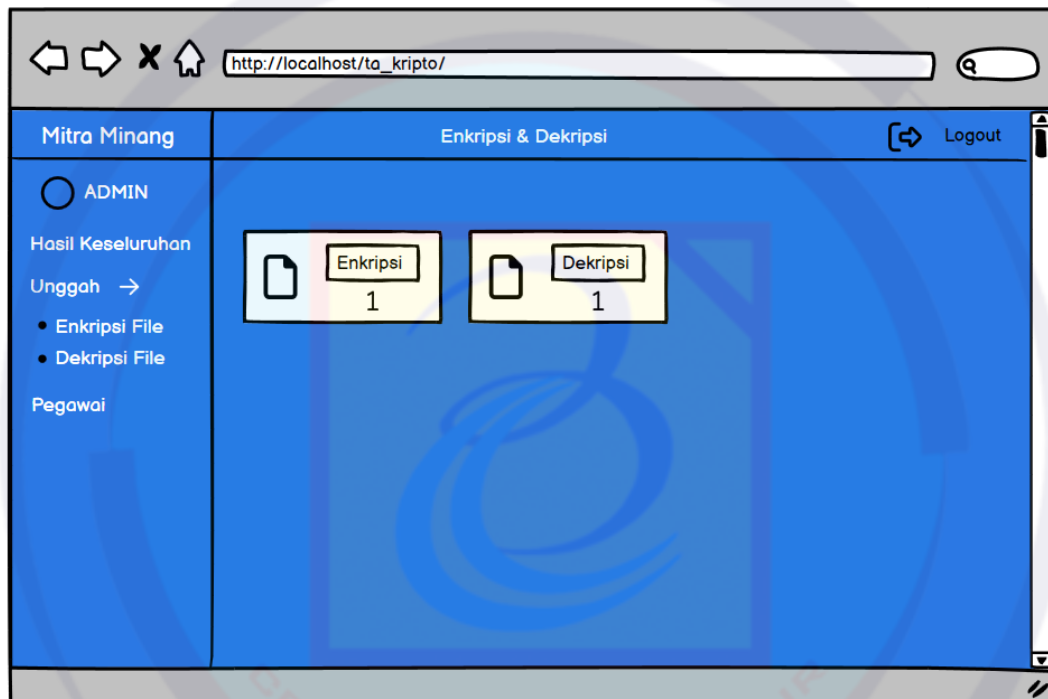
### 3.7.2 Rancangan Layar Pada Menu Awal

Setelah pengguna memasuki program aplikasi, rancangan halaman utama ini menampilkan tampilan awal. Pada tampilan ini dibagi menjadi dua tergantung pada pengguna.

#### a. Tampilan Menu Hasil Keseluruhan Pada Admin

Pada tampilan ini terdapat tiga menu, yaitu hasil keseluruhan, unggah *file* (enkripsi dan dekripsi), pegawai.

Berikut adalah tampilan layar pada menu utama untuk *admin* :

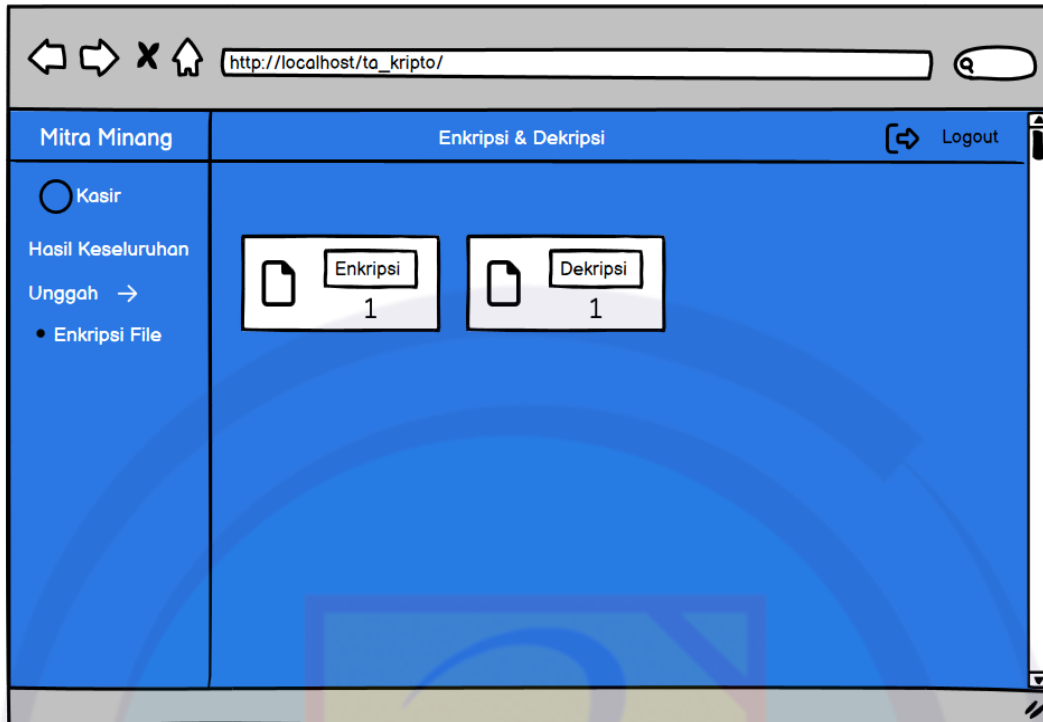


Gambar 3. 4 Tampilan rancangan layar pada menu awal *admin*

#### b. Tampilan Menu *Dashboard* Pada Pegawai atau Kasir

Pada tampilan ini terdapat dua menu, yaitu hasil keseluruhan, unggah *file* (enkripsi). Yang hanya membedakan adalah tidak ada menu dekripsi dan menu pegawai.

Berikut adalah tampilan layar pada menu utama untuk pegawai atau kasir :



Gambar 3. 5 Tampilan rancangan layar pada menu awal pegawai atau kasir

### 3.7.3 Rancangan Layar Pada Menu Unggah File

Pada tampilan ini untuk pengguna *admin* dan pegawai atau kasir memiliki perbedaan, yaitu pada pengguna *admin* mempunyai menu enkripsi *file* dan dekripsi *file*, sedangkan untuk pengguna pegawai atau kasir hanya mempunyai menu enkripsi *file* saja. Tampilan menu enkripsi *file* pada sistem untuk *admin* dan kasir memainkan peran penting dalam menjaga keamanan informasi. Dengan memasukkan *password* yang tepat, pengguna *admin* dapat mengakses menu untuk mengenkripsi atau mendekripsi data yang sebelumnya di enkripsi oleh pegawai atau kasir. Proses ini tidak hanya memastikan keamanan data yang disimpan, tetapi juga memungkinkan pemilik untuk mengelola informasi dengan lebih efektif.

#### a. Tampilan Menu Enkripsi File Pada Admin dan Pegawai atau Kasir

Pada tampilan menu ini pengguna *admin* maupun pegawai atau kasir sama-sama diminta untuk memasukan *file* yang telah disiapkan dan setelah itu masing-masing pengguna diminta untuk memasukan *password* serta keterangan deskripsi.



Berikut adalah tampilan layar pada menu enkripsi *file* untuk *admin* dan pegawai atau kasir :

Browser address bar: [http://localhost/ta\\_kripto/](http://localhost/ta_kripto/)

Page Header: Enkripsi & Dekripsi [Logout]

Left Sidebar: Mitra Minang  
● ADMIN  
Hasil Keseluruhan  
Unggah →  
• Enkripsi File  
• Dekripsi File  
Pegawai

Main Content: Proses Enkripsi

Form Fields:

- File:
- Password:
- Keterangan:

Enkripsi File

Gambar 3. 6 Tampilan rancangan layar pada menu enkripsi *admin*

Browser address bar: [http://localhost/ta\\_kripto/](http://localhost/ta_kripto/)

Page Header: Enkripsi & Dekripsi [Logout]

Left Sidebar: Mitra Minang  
● KARYAWAN  
Hasil Keseluruhan  
Unggah →  
• Enkripsi File

Main Content: Proses Enkripsi

Form Fields:

- File:
- Password:
- Keterangan:

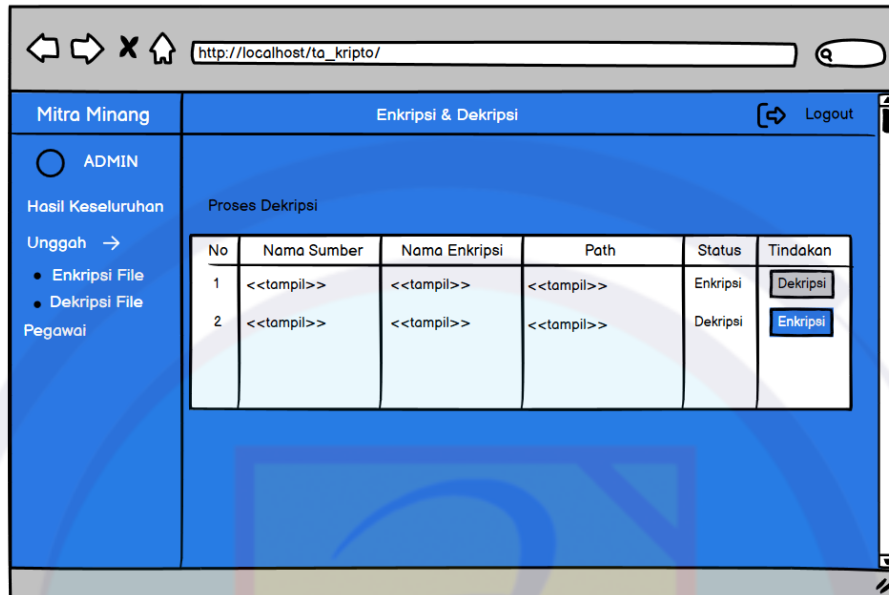
Enkripsi File

Gambar 3. 7 Tampilan rancangan layar pada menu enkripsi pegawai atau kasir

**b. Tampilan Menu Dekripsi *File* Pada *Admin***

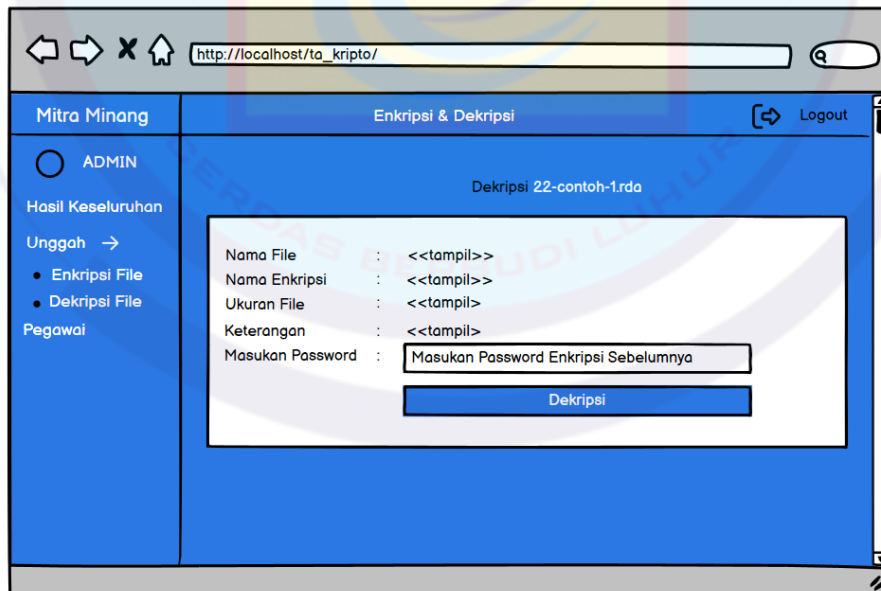
Pada tampilan menu ini pengguna *admin* diminta untuk memasukkan *password* yang sebelumnya sudah dimasukan pada *file* yang telah dienkrapsikan.

Berikut adalah tampilan layar pada menu dekripsi *admin* :



**Gambar 3. 6 Tampilan rancangan layar pada menu dekripsi *admin***

Berikut adalah tampilan layar pada submenu dekripsi *admin* :

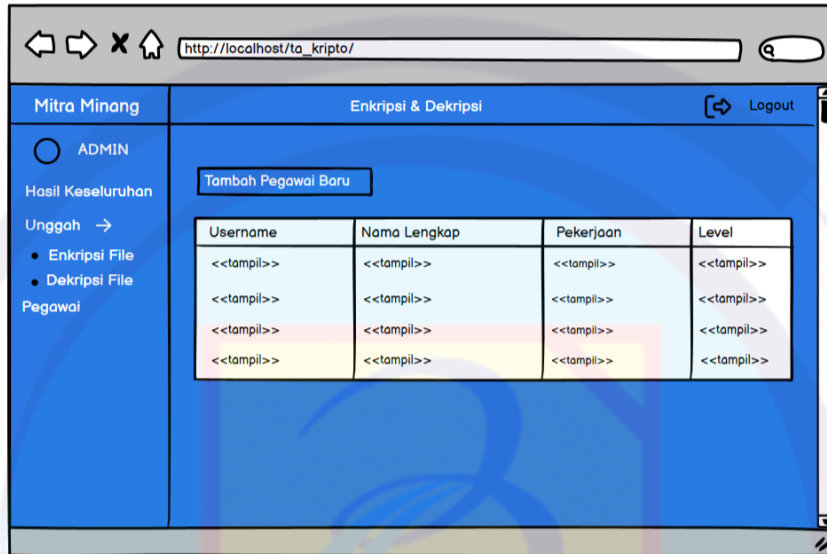


**Gambar 3. 7 Tampilan rancangan layar pada submenu dekripsi *admin***

### 3.7.4 Rancangan Layar Pada Menu Pegawai Pengguna Admin

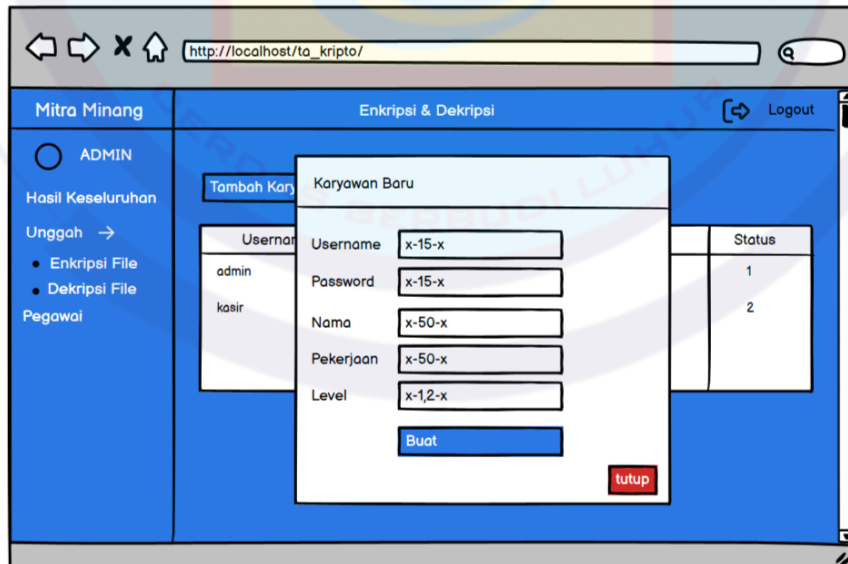
Pada tampilan ini menampilkan menu pegawai yang hanya ada di pengguna sebagai *admin*, dimana *admin* dapat melihat daftar pegawai mana saja yang sudah terdaftar dan dapat menambahkan pegawai baru pada submenu “TAMBAH PEGAWAI BARU”, lalu akan muncul *popup* dan pengguna diminta untuk memasukkan *username*, *password*, nama, pekerjaan, dan status.

Berikut adalah tampilan layar pada menu pegawai pengguna *admin* :



Gambar 3. 8 Tampilan rancangan layar pada menu pegawai pengguna *admin*

Berikut adalah tampilan layar pada *submenu* pegawai pengguna *admin* :



Gambar 3. 9 Tampilan rancangan layar pada *submenu* pegawai *admin*

## BAB IV

### HASIL DAN PEMBAHASAN

#### 4.1 Lingkungan Percobaan

Untuk percobaan yang dilakukan, telah disiapkan dua komponen penting hardware dan software yang akan digunakan untuk implementasi. Spesifikasi kedua komponen tersebut harus ditetapkan dengan tujuan untuk mendukung proses percobaan, yang diharapkan berjalan dengan baik dan menghasilkan hasil yang memuaskan. Sesuai apa yang diinginkan.

Spesifikasi sistem menjelaskan persyaratan operasional dan kinerja suatu sistem, seperti komputer. Pedoman operasional dan kinerja program aplikasi ditentukan dengan bantuan spesifikasi sistem.

##### 4.1.1 Spesifikasi Perangkat Keras

Pada penerapan algoritma AES-128 pada metode kriptografi membutuhkan perangkat keras yang bisa menjalankan sistem, Sebagai sarana pendukung utama. Spesifikasi perangkat keras yang digunakan pada penelitian ini bisa dilihat pada tabel 4.1.

**Tabel 4. 1 Spesifikasi Perangkat keras**

No	Komponen	Spesifikasi
1	<i>Processor</i>	AMD Ryzen 7
2	RAM	16 GB
3	<i>Penyimpanan</i>	500 GB
4	<i>Keyboard</i>	
5	<i>Mouse</i>	
6	<i>Monitor</i>	

##### 4.1.2 Spesifikasi Perangkat Lunak

Tujuan, deskripsi kebutuhan, dan persiapan validasi aplikasi perangkat lunak termasuk dalam tahap spesifikasi perangkat lunak. Perangkat lunak sebagai alat non-fisik sangat penting untuk hasil keluaran. Spesifikasi perangkat lunak yang digunakan pada penelitian ini bisa dilihat pada tabel 4.2.

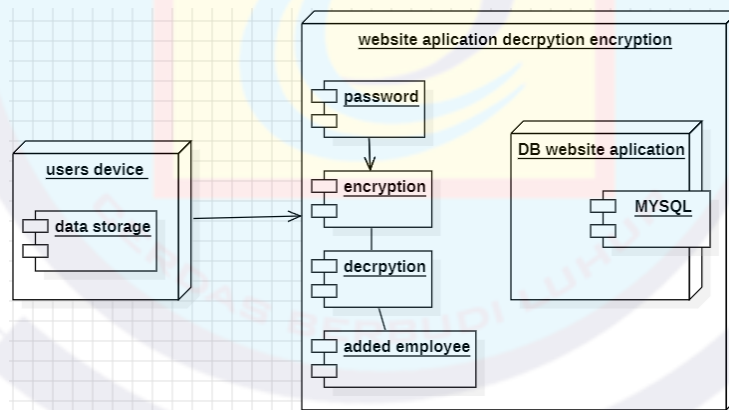
Tabel 4. 2 Spesifikasi perangkat lunak

No	Komponen	Spesifikasi
1	Sistem Operasi	Windows 11
2	Program	PHP
3	<i>Editor</i>	Visual Studio Code
4	<i>Software</i>	XAMPP v3.2.2
5	<i>Database</i>	Phpmyadmin dan Mysql

#### 4.1.3 Deployment Diagram

Gambar alur tahapan proses pengguna yang digunakan untuk enkripsi dan dekripsi aplikasi ditampilkan di *deployment diagram* ini. Dari data penyimpanan komputer lalu pengguna mengupload *file* yang telah disiapkan sebelumnya untuk dienkripsi. Kemudian pengguna diminta untuk mengisi *password* untuk file yang dienkripsi. Pada *file* yang telah dienkripsi pengguna juga bisa mengembalikannya lagi dengan menggunakan menu dekripsi, kemudian pengguna diminta untuk mengisi *password* kembali dengan menggunakan *password* yang sama sesuai dengan *file* yang dienkripsi sebelumnya. Disini *password* juga digunakan untuk penambahan pengguna maupun *admin* ataupun pegawai.

Berikut tahapan gambar *deployment diagram*



Gambar 4. 1 Deployment Diagram

#### 4.2 Implementasi Metode

Program ini berfokus pada menu yang memungkinkan pengguna mengenkripsi algoritma AES, ada proses enkripsi yang melibatkan empat jenis perubahan byte *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Pada tahap pertama enkripsi, input yang telah disalin ke 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.

### 4.3 Flowchart

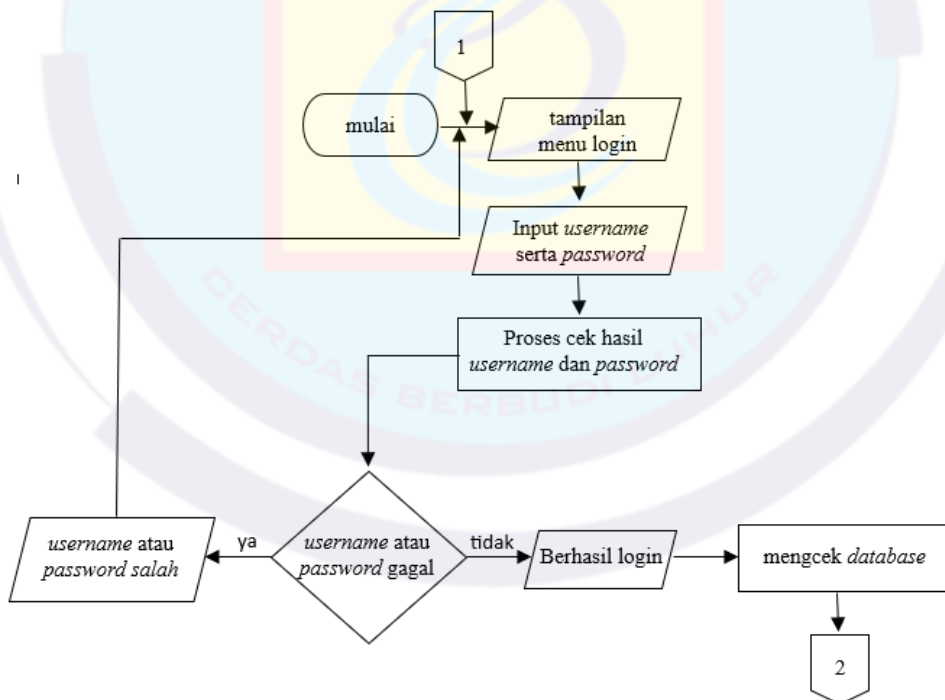
Pada awal aplikasi dimulai, maka menu yang akan terlebih muncul adalah menu *login*, memungkinkan hanya pengguna yang telah terdaftar oleh *admin* untuk mengakses dan menjalankan program tersebut. Setelah *login* pengguna akan masuk kehalaman utama yang telah diatur sesuai dengan status *level* dari pengguna.

Program ini berfokus pada menu yang memungkinkan pengguna mengenkripsi dan mendekripsi dokumen. Ini memungkinkan pemilik data agar dapat melindungi dokumen pengguna dengan metode enkripsi dan dekripsi AES-128.

#### 4.3.1 Flowchart Menu Login

Untuk menjaga agar tidak ada orang lain yang dapat menggunakan program ini, pada tampilan pertama yang dilihat pengguna adalah menu *login* ini, yang digunakan untuk masuk ke program untuk digunakan. Sebab hanya pengguna saja yang bisa menggunakan program ini yang sudah terdaftar di *database* dengan cara memasukan *username* dan *password*.

Berikut adalah tahapan pada proses *login* :



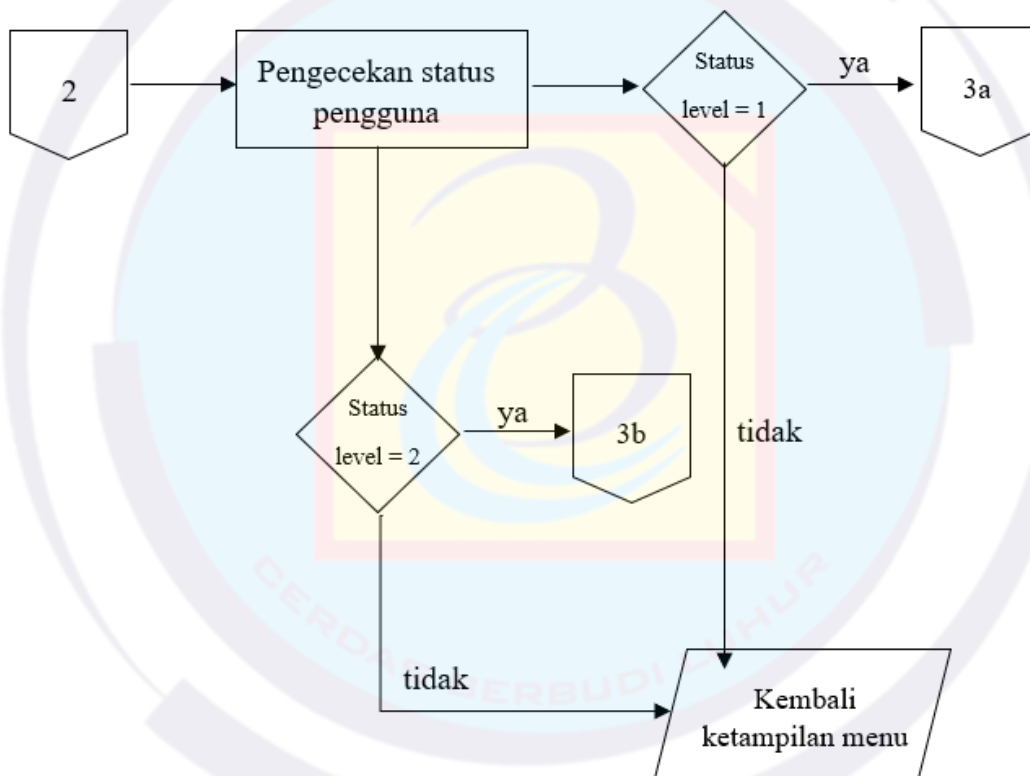
Gambar 4. 2 Flowchart tahapan menu login



#### 4.3.2 Flowchart Menu Level Status Pengguna

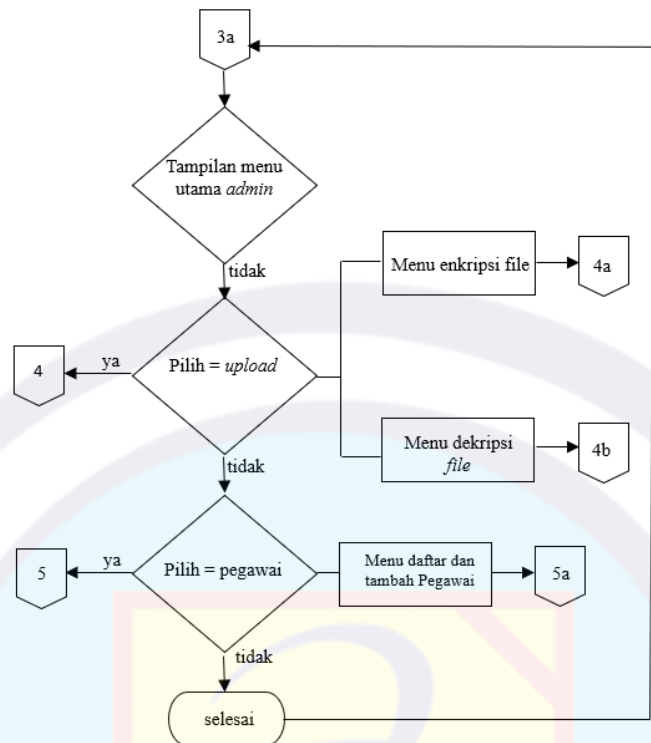
Dalam sistem kriptografi leveling ini, *level* status 1 bertindak sebagai *admin* yang memiliki akses penuh terhadap fungsi enkripsi dan dekripsi. Mereka dapat mengamankan suatu *file* dengan mengenkripsi *file* sensitif dan mendekripsinya kembali saat diperlukan. Sebaliknya, *level* status 2 sebagai pegawai atau kasir hanya diberikan akses untuk melakukan proses enkripsi. Hal ini dapat mengamankan data dengan mengubahnya menjadi format terenkripsi, tetapi tidak memiliki kemampuan untuk mengembalikan data tersebut ke bentuk aslinya. Dengan membatasi fungsi dekripsi hanya pada *level* pengguna *admin*, sistem ini memastikan kontrol keamanan yang ketat dan mempertahankan integritas informasi yang sensitif.

Berikut adalah tahapan pada proses pengguna status *leveling* :



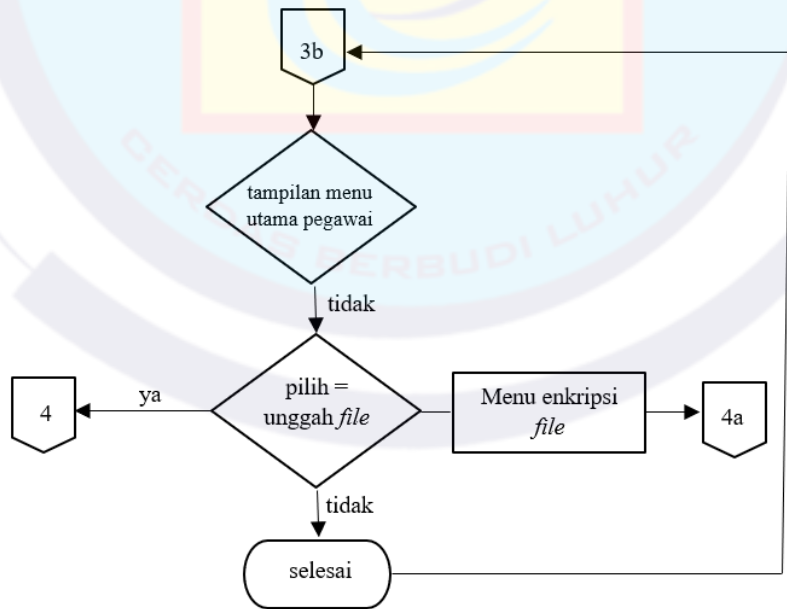
Gambar 4. 3 Flowchart tahapan *level* status pengguna

Berikut adalah tahapan pada proses pengguna *admin* :



Gambar 4. 4 Flowchart tahapan level pengguna admin

Berikut adalah tahapan pada proses pengguna pegawai :

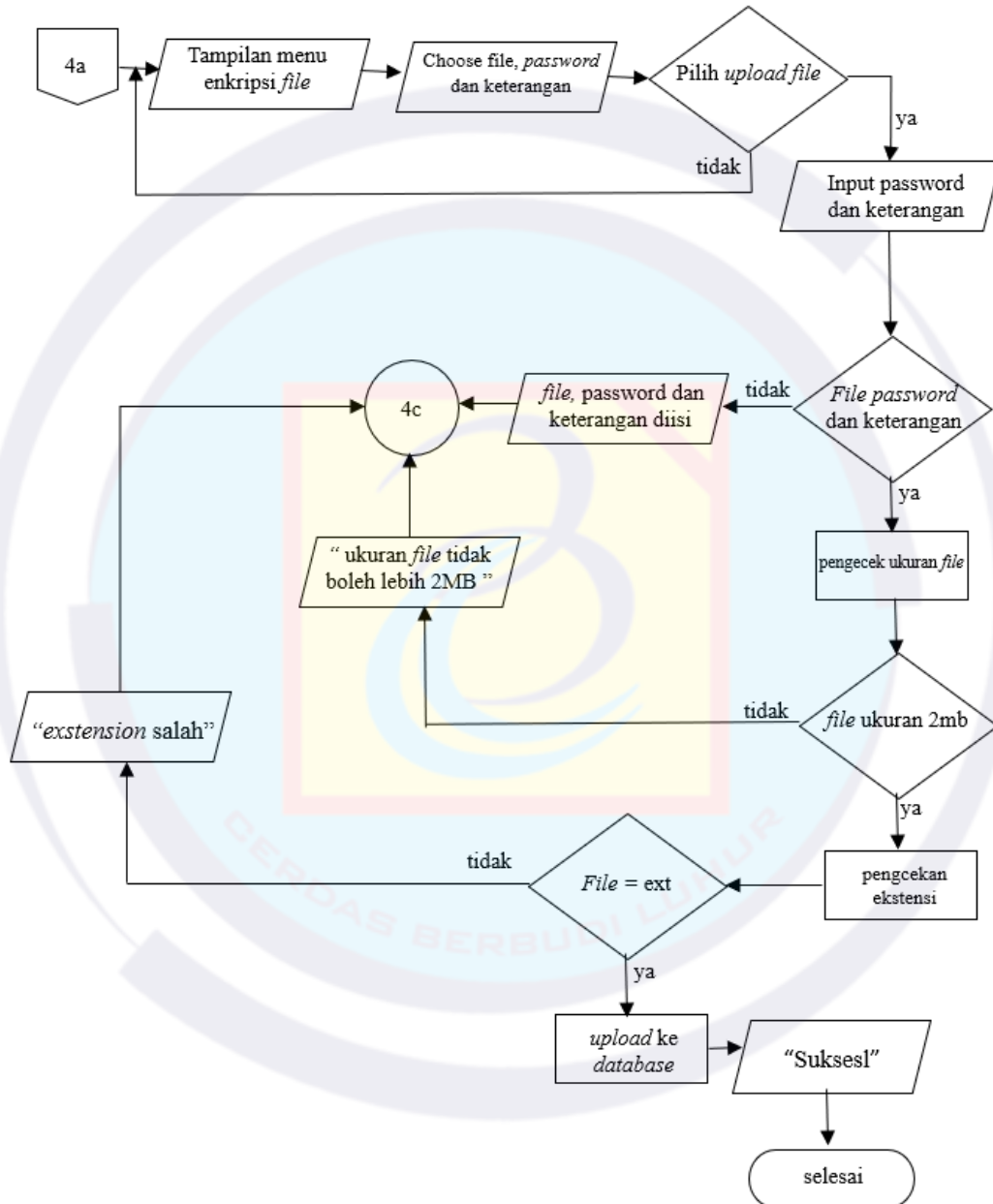


Gambar 4. 5 Flowchart tahapan level pengguna pegawai

### 4.3.3 Flowchart Pada Proses Enkripsi

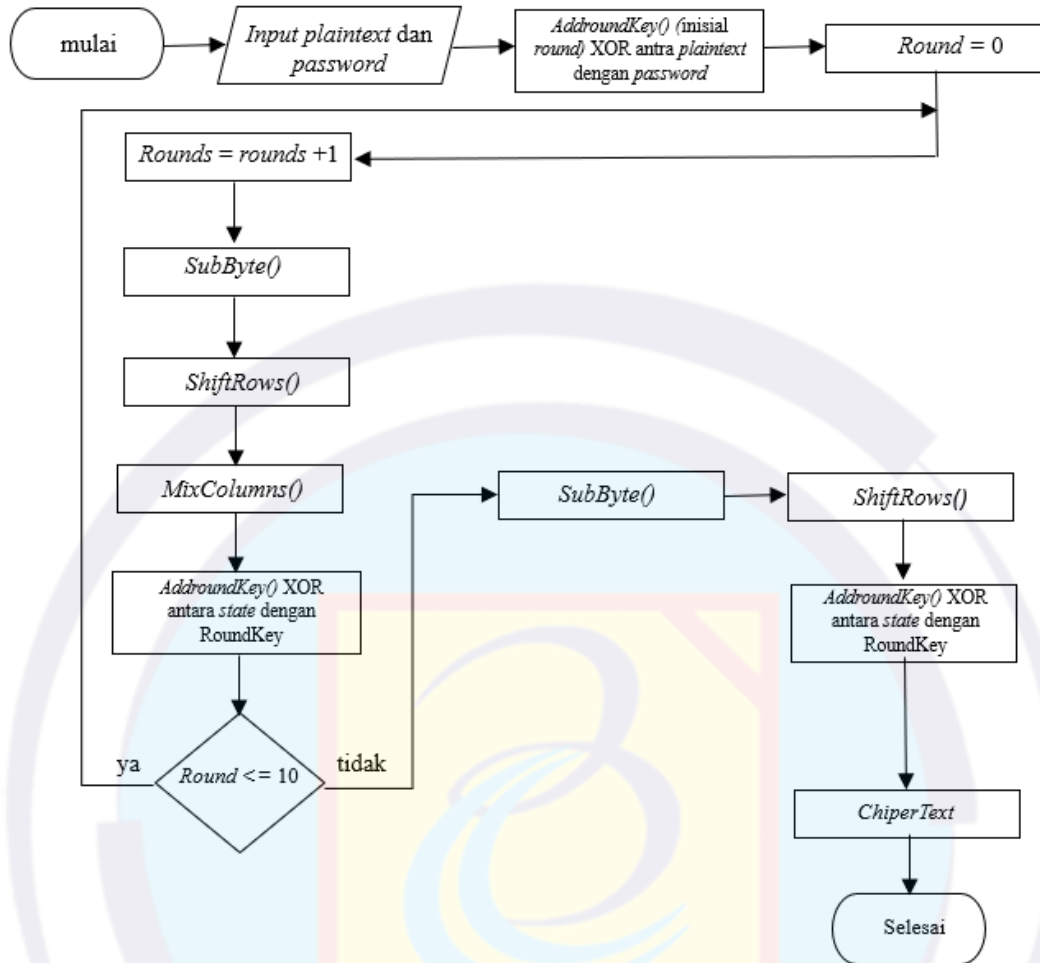
Pada dalam suatu proses enkripsi AES-128 pada masing-masing tipe yang menggunakan kunci internal yaitu, *AddRoundKey* digunakan untuk pada setiap putaran pada prosesnya. Proses enkripsi AES-128 diputar sepuluh kali ( $a=10$ ).

Berikut adalah tahapan pada proses *upload file* enkripsi :



Gambar 4. 6 Flowchart tahapan menu *upload file* untuk enkripsi

Berikut adalah tahapan pada proses enkripsi AES-128 :



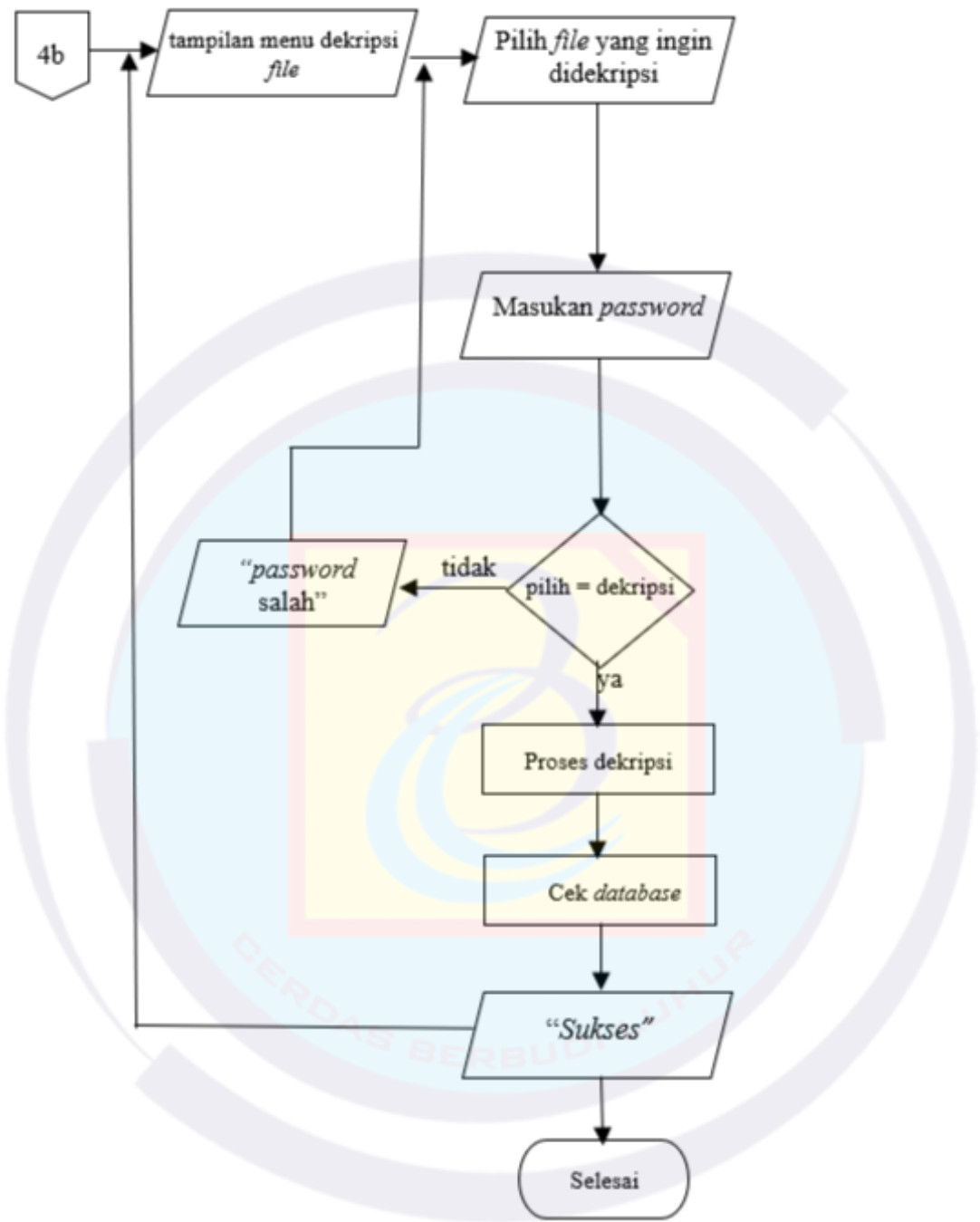
Gambar 4. 7 Flowchart tahapan proses pada enkripsi

#### 4.3.4 Flowchart Pada Proses Dekripsi Pengguna Admin

Setelah itu selanjutnya sesudah memilih menu pada dekripsi di menu unggah *file* maka selanjutnya, pengguna yaitu *admin* dapat melihat *file* dokumen yang akan ingin didekripsikan. Untuk bisa dapat melanjutkan proses pada dekripsi maka dibutuhkan kata sandi yang sama pada proses enkripsi *file* sebelumnya untuk bisa mendekripsikannya.

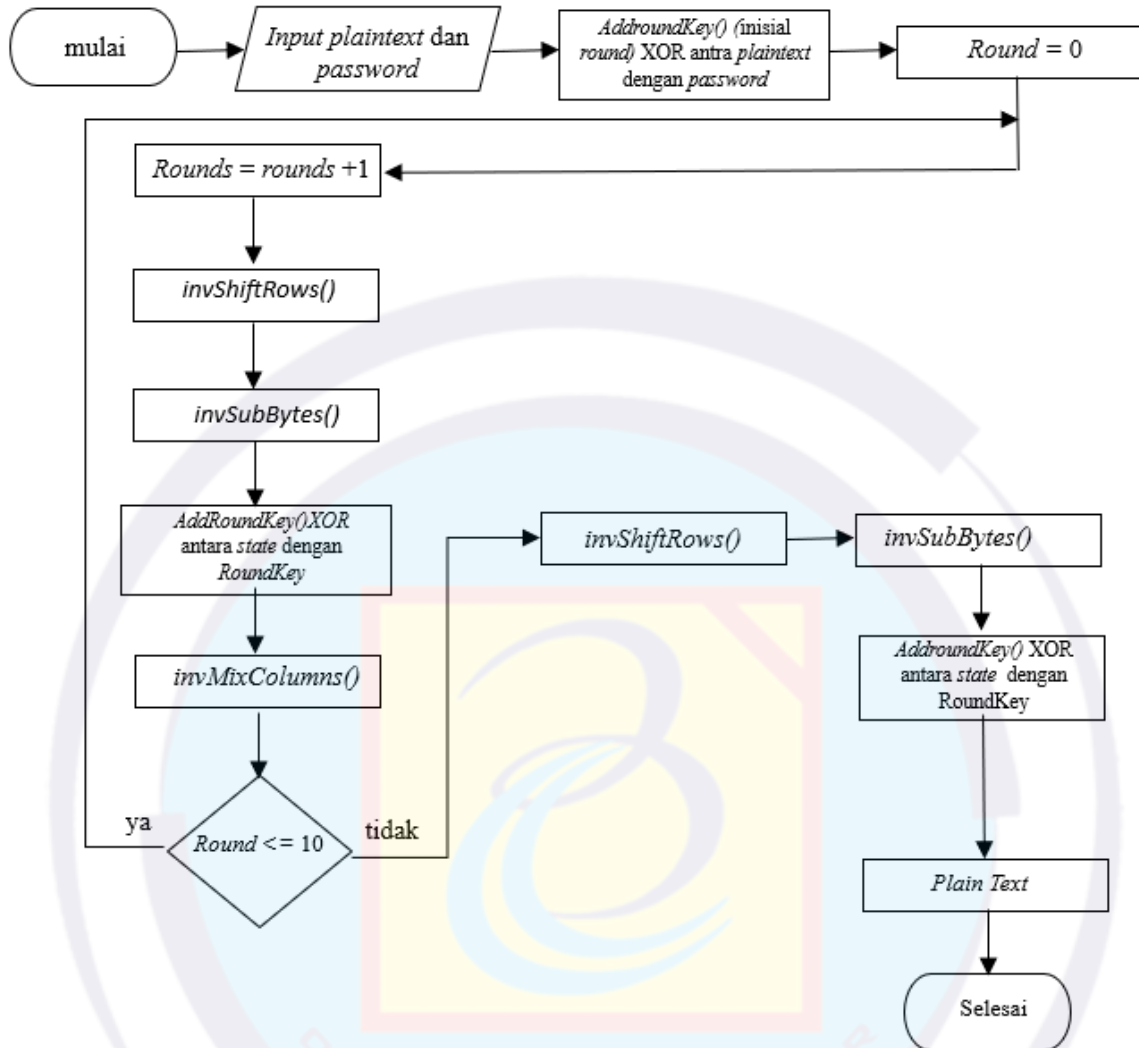
Pada saat proses dekripsi AES-128 prosesnya juga dilakukan sebanyak sepuluh kali ( $a=10$ ), tetapi dengan perhitungan *invers*.

Berikut adalah tahapan pada proses dekripsi file :



Gambar 4. 8 Flowchart tahapan proses pada menu dekripsi

Berikut adalah tahapan pada proses dekripsi AES-128 :



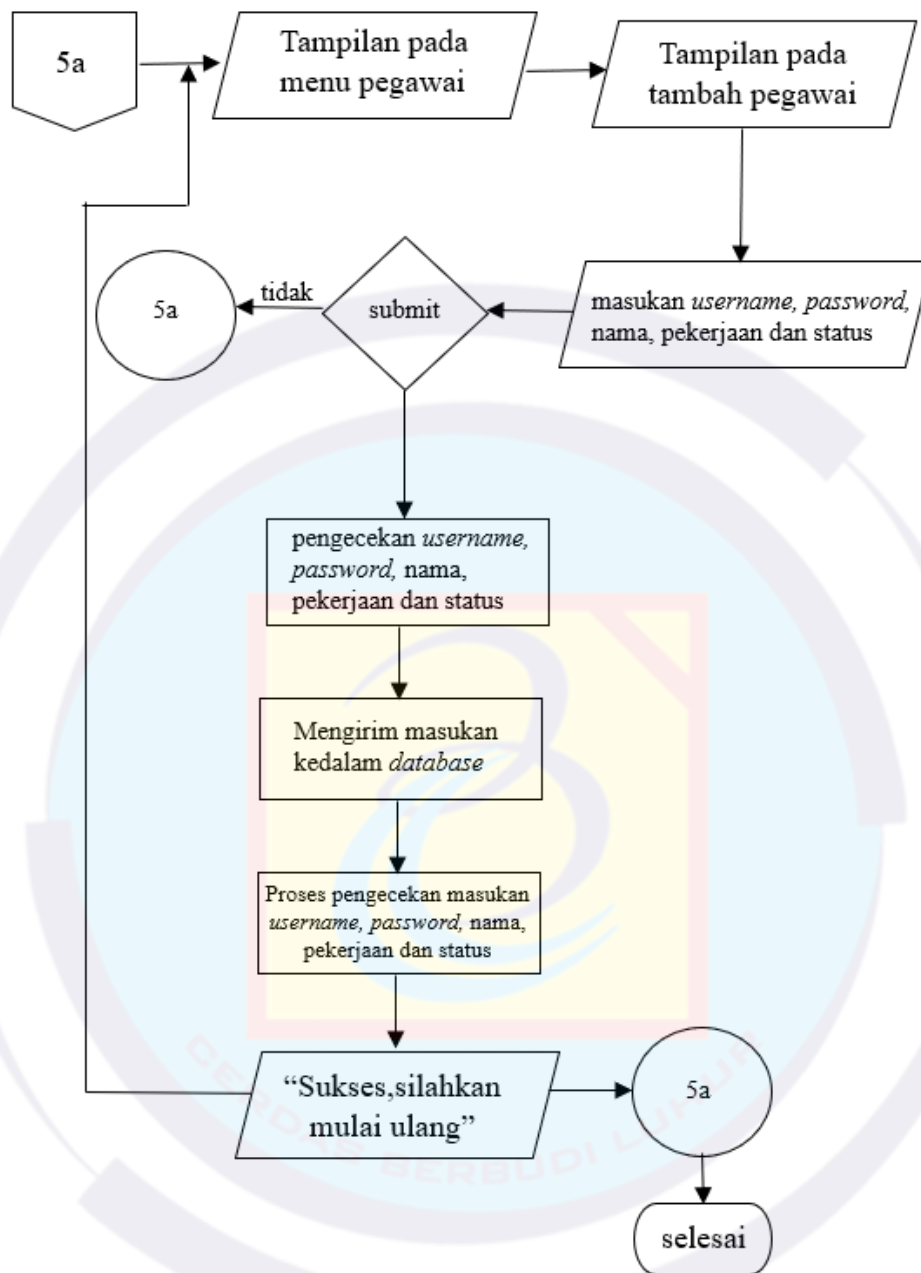
Gambar 4. 9 Flowchart tahapan proses pada dekripsi

#### 4.3.5 Flowchart Pada Menu Pegawai

Selanjutnya tujuan pada tahap ini adalah untuk memungkinkan *admin* untuk mendaftarkan pegawai baru pada aplikasi enkripsi *file* dan dekripsi *file*. Oleh karena itu hanya pada pengguna *admin* ini saja dimenu pegawai ini yang hanya dapat menggunakan menu tersebut. Untuk memberikan akses keaplikasi enkripsi *file* dan dekripsi *file* ini, *admin* juga dapat mengisikan *admin* terbaru dalam menu ini.



Berikut adalah proses menu pegawai :



Gambar 4. 10 Flowchart tahapan pada menu pegawai

#### 4.4 Algoritma

Pada tahap bagian ini memperlihatkan proses algoritma dalam bahasa pemrograman enkripsi *file* dan dekripsi *file*.

Berikut adalah proses pemrograman enkripsi :

```
Start
  Input Plaintext dan Kunci
  AddRoundKey1 = Plaintext XOR
  Kunci
  Round = 0
  Round = Round + 1
  SubBytes()
  ShiftRowsl()
  MixColumns0()
  AddRoundKey() = Current State XOR
  Round Key
  if Rounds <= 10 Then
  Else
    Kembali ke baris 5
  SubBytes()
  ShiftColumn0()
  AddRoundKey0 = Current
  State XOR Round Key
  Output Chiphertext
Endif
End
```

Gambar 4. 11 program proses enkripsi

Berikut adalah proses pemrograman dekripsi :

```
Start
  Input Ciphertext dan Kunci
  AddRoundkey() = Ciphertext XOR
  Kunci
  Password
  Rounds = 0
  Rounds = Rounds + 1 Proses
  InvshiftRows()Proses InvsSubBytes()
  Proses AddRoundKey() =current
  State
  XOR Round Key
  Proses InvMixColumns()
  if Rounds <= 10 Then
    Kembali ke baris 5
  Else
    Proses InvshiftRows()
    Proses InvsSubBytes()
    Proses AddRoundKey()
    Proses AddRoundKey() =current
  State
  XOR Round Key
  Endlf
End
```

Gambar 4. 12 program proses dekripsi


## 4.5 Pengujian

Selanjutnya setelah semua aspek terpenuhi maka proses selanjutnya yaitu, pada tahap pengujian.

### 4.5.1 Pengujian Enkripsi

Pada saat melakukan enkripsi, pengguna bisa melakukannya seperti yang dijelaskan sebelumnya. Pengguna diminta untuk memilih *file* yang sebelumnya telah disiapkan, lalu pengguna dimintai *password* setelah itu klik tombol enkripsi.

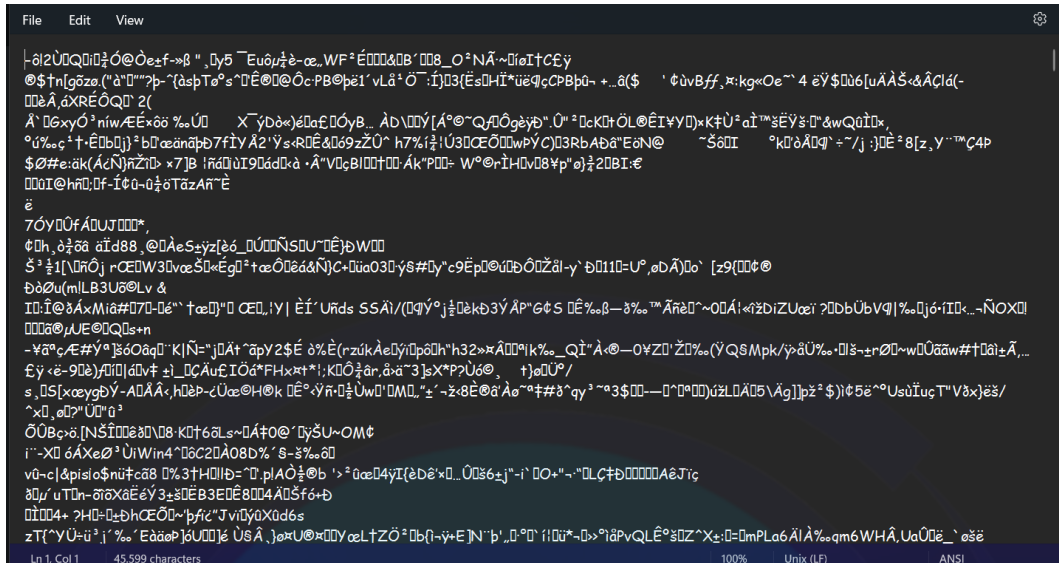
Berikut contoh *file* xlsx yang digunakan :

	A	B	C	D	E
1					
2		NOTA PENJUALAN			
3		 Jl. Ir. H. Juanda No.21 1, RT.14/RW.4, Kb. Klp., Kecamatan Gambir, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10120			
4		JAKARTA			
5					
6	No	: 081318367038		Tanggal	: 24 mei 24
7	Nama	: rismawan		Nomor	:
8					
9	No	Pesanan	Jumlah	Harga	Total
10	1	Nasi ayam cabe ijo	10	17 ribu	170 ribu
11	2	Nasi telur dadar	6	13 ribu	78 ribu
12					
13					
14					
15					
16					
17					
18					
19					
20				Jumlah	248 ribu
21				Uang	300 ribu
22				Kembalian	52 ribu
23					
24					
25				Hormat	
26					
27					
28					

Gambar 4. 13 Contoh *file* xlsx asli nota penjualan sebelum dienkrpsi

Setelah *file* berhasil dienkrpsi maka *file* yang telah dienkrpsi akan berubah format yang tidak dikenali.

Berikut adalah tampilan *file* yang telah dienkripsi :



Gambar 4. 14 Contoh *file* xlsx asli nota penjualan setelah dienkripsi

Apabila *file* ingin dikembalikan kembali seperti semula maka pengguna diminta untuk menggunakan menu dekripsi dengan cara memilih *file* yang ingin didekripsi lalu pengguna diminta untuk memasukkan kembali *password* yang sebelumnya digunakan untuk mengenkripsi *file* sebelumnya. Maka *file* akan kembali seperti tampilan awal.

#### 4.5.2 Kesimpulan Hasil Uji Coba Enkripsi dan Dekripsi

Pada aplikasi yang telah dibuat ini merupakan pembelajaran aplikasi pengamanan data dengan menggunakan algoritma AES. Dengan adanya aplikasi ini pengguna dapat mengamankan *file* penting, sehingga *file* yang bersifat rahasia tetap terjaga dan utuh sehingga keamanan *file* terjamin keamanannya.

Adapun tabel pengujian enkripsi dan dekripsi pada aplikasi ini. Yang bisa dilihat pada tabel 4.3 ini.

Tabel 4. 3 Hasil uji coba enkripsi

No	Nama <i>File</i>	Ukuran <i>File</i>	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

No	Nama File	Ukuran File	Waktu Dibutuhkan
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

Berikut tabel pengujian enkripsi dan dekripsi pada aplikasi ini. Yang bisa dilihat pada tabel 4.4 ini.

Tabel 4. 4 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

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.

Tabel 4. 5 Tabel hasil uji coba aplikasi

NO	Aktivitas Pengujian	Realisasi yang diharapkan	Hasil Pengujian	Kesimpulan
1	<i>login</i>	menguji <i>username</i> dan <i>password</i> untuk melakukan <i>login</i>	berhasil lalu masuk kehalaman utama	diterima
2	<i>user</i> mengklik tombol menu unggah <i>file</i>	untuk melakukan proses enkripsi <i>file</i> dan dekripsi <i>file</i>	berhasil memilih melakukan enkripsi <i>file</i> atau dekripsi <i>file</i>	diterima
3	<i>user</i> mengklik tombol enkripsi <i>file</i> pada menu unggah <i>file</i>	untuk melakukan proses enkripsi pada <i>file</i>	berhasil masuk kedalam halaman enkripsi <i>file</i>	diterima
4	<i>user</i> mengklik uoload <i>file</i>	untuk <i>user</i> bisa mengupload <i>file</i> yang ingin dienkripsi	muncul <i>popup file explorer</i> pada <i>user</i> untuk memilih <i>file</i>	diterima
5	<i>user</i> mengklik tombol enkripsi	setelah mengisi <i>password</i> dan keterangan lalu menguji <i>file</i> yang ingin dienkripsi	enkripsi yang dilakukan berhasil	diterima
6	<i>user</i> mengklik tombol dekripsi <i>file</i> pada menu unggah <i>file</i>	untuk melakukan proses enkripsi pada <i>file</i>	berhasil masuk kedalam halaman dekripsi	diterima
7	<i>user</i> mengklik tombol dekripsi	setelah mengisi <i>password</i> yang sama seperti awal enkripsi lalu menguji <i>file</i> yang ingin didekripsi	dekripsi yang dilakukan berhasil	diterima
8	<i>user</i> mengklik tombol pegawai	untuk melihat dan menambahkan profil pegawai	berhasil melihat profil pegawai	diterima
9	<i>user</i> mengklik tombol tambah pegawai baru	untuk menambah pegawai baru diminta untuk mengisi profil yang disediakan	muncul <i>popup</i> untuk menambahkan pegawai baru	diterima



NO	Aktivitas Pengujian	Realisasi yang diharapkan	Hasil Pengujian	Kesimpulan
10	<i>user</i> mengklik tombol buat pada tambah pegawai	uji penambahan pegawai	berhasil terdaftar	diterima

## 4.6 Tampilan Layar Aplikasi

Implementasi antar muka adalah proses membuat antar muka pada sistem sesuai dengan rancangan tampilan yang sudah dibuat pada tahap sebelumnya. Berikut tampilan antarmuka dalam sistem pengamanan data transaksi penjualan dan pembelian Rumah Makan Mitra Minang. Untuk Mengetahui tampilan layar aplikasi enkripsi dan dekripsi dari awal pengoperasian hingga akhir pengoperasian dibahas pada bagian ini.

### 4.6.1 Menu Halaman *Login Admin* dan Pegawai

Pada tahap ini 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.

Berikut adalah menu halaman *login admin* dan pegawai atau kasir :



Gambar 4. 15 Menu halaman *login admin* dan pegawai

#### 4.6.2 Menu Halaman Utama Admin dan Pegawai

Setelah berhasil *login* setelah itu akan masuk kedalam menu utama yaitu menu *dashboard*. Pada menu *dashboard* ini berada dihalaman utama pada aplikasi ini. Pengguna dapat melihat jumlah hasil dokumen yang dienkripsi dan sudah yang didekripsi di menu utama ini. Di dalam menu ini untuk pengguna *admin* memiliki menu *upload file* yang didalamnya mempunyai menu enkripsi dan menu dekripsi yang bertujuan untuk mengamankan serta mengembalikan *file* yang telah diamankan, selanjutnya menu pegawai yang berfungsi untuk melihat daftar pegawai dan terdapat submenu untuk menambahkan pegawai baru.

Berikut adalah menu halaman utama *admin* :



Gambar 4. 16 Menu halaman awal *admin*

Berikut adalah menu halaman utama pegawai :



Gambar 4. 17 Menu halaman awal pegawai atau kasir

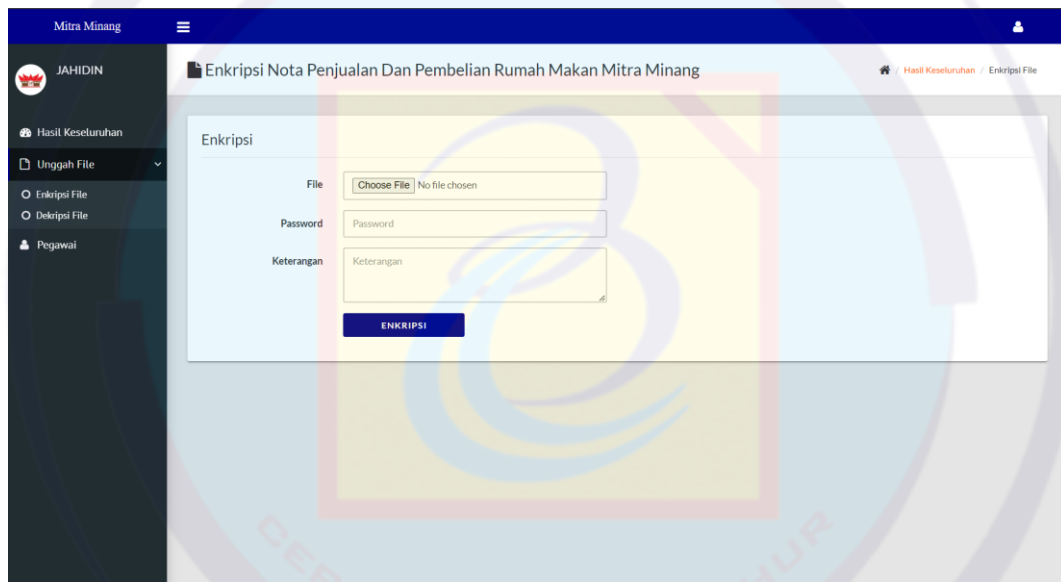
#### 4.6.3 Menu Halaman Unggah File Admin dan Kasir

Pada tahap menu ini, menu *upload file* masing-masing pengguna *admin* dan pegawai mempunyai perbedaan yaitu, pada pengguna *admin* mempunyai dua submenu enkripsi *file* dan dekripsi *file*, sedangkan pada pengguna pegawai atau kasir hanya mempunyai satu submenu enkripsi *file* saja.

##### a. Menu Halaman Unggah File Admin dan Pegawai (Enkripsi)

Pada 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.

Berikut adalah menu halaman unggah *file* dengan submenu enkripsi pada *admin* dan pegawai :

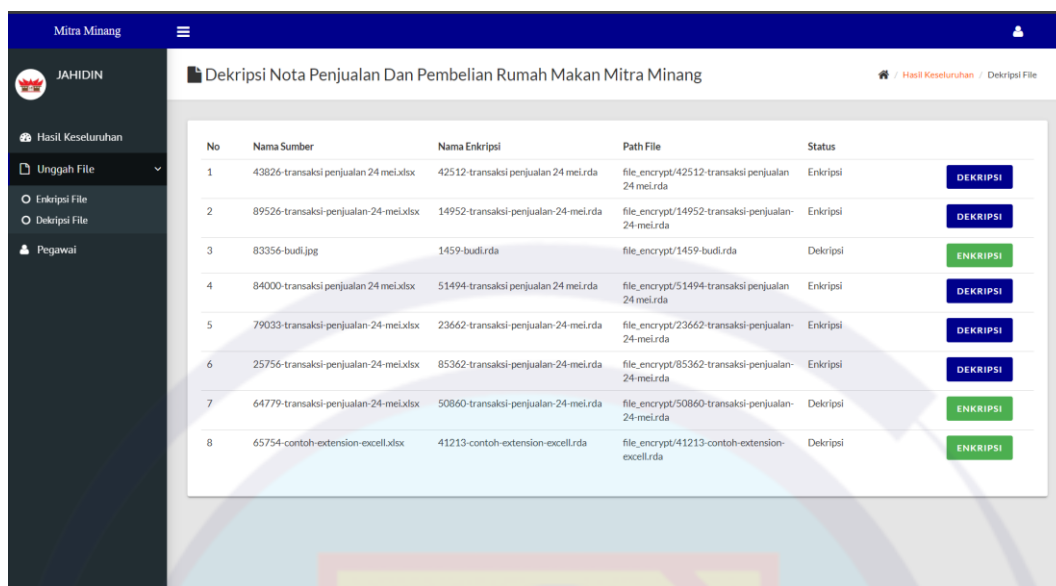


Gambar 4. 18 Menu halaman enkripsi *admin* dan pegawai

##### b. Menu Halaman Upload File Admin (Dekripsi)

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.

Berikut adalah menu halaman *upload file* dengan *submenu* dekripsi *file* pada *admin* :



No	Nama Sumber	Nama Enkripsi	Path File	Status
1	43826-transaksi penjualan 24 mei.xlsx	42512-transaksi penjualan 24 mei.rda	file_encrypt/42512-transaksi penjualan 24 mei.rda	Enkripsi
2	89526-transaksi-penjualan-24-mei.xlsx	14952-transaksi-penjualan-24-mei.rda	file_encrypt/14952-transaksi-penjualan-24-mei.rda	Enkripsi
3	83356-budi.jpg	1459-budi.rda	file_encrypt/1459-budi.rda	Dekripsi
4	84000-transaksi penjualan 24 mei.xlsx	51494-transaksi penjualan 24 mei.rda	file_encrypt/51494-transaksi penjualan 24 mei.rda	Enkripsi
5	79033-transaksi-penjualan-24-mei.xlsx	23662-transaksi-penjualan-24-mei.rda	file_encrypt/23662-transaksi-penjualan-24-mei.rda	Enkripsi
6	25756-transaksi-penjualan-24-mei.xlsx	85362-transaksi-penjualan-24-mei.rda	file_encrypt/85362-transaksi-penjualan-24-mei.rda	Enkripsi
7	64779-transaksi-penjualan-24-mei.xlsx	50860-transaksi-penjualan-24-mei.rda	file_encrypt/50860-transaksi-penjualan-24-mei.rda	Dekripsi
8	65754-contoh-extension-excel.xlsx	41213-contoh-extension-excel.rda	file_encrypt/41213-contoh-extension-excel.rda	Dekripsi

Gambar 4. 19 Menu halaman dekripsi *file* pada *admin*

Berikut adalah menu halaman proses dekripsi *file* pada menu unggah *file* dengan *submenu* dekripsi *file* pada *admin* :



Dekripsi File: 42512-transaksi penjualan 24 mei.rda

Nama Sumber	:	43826-transaksi penjualan 24 mei.xlsx
Nama Enkripsi	:	42512-transaksi penjualan 24 mei.rda
Ukuran File	:	15784 KB
Keterangan	:	123
Password	:	<input type="password" value="Masukan Password Enkripsi Sebelumnya"/>

**DEKRIPSI**

Gambar 4. 20 Menu halaman proses dekripsi *file* pada *admin*

#### 4.6.4 Menu Halaman Pegawai Pada Admin

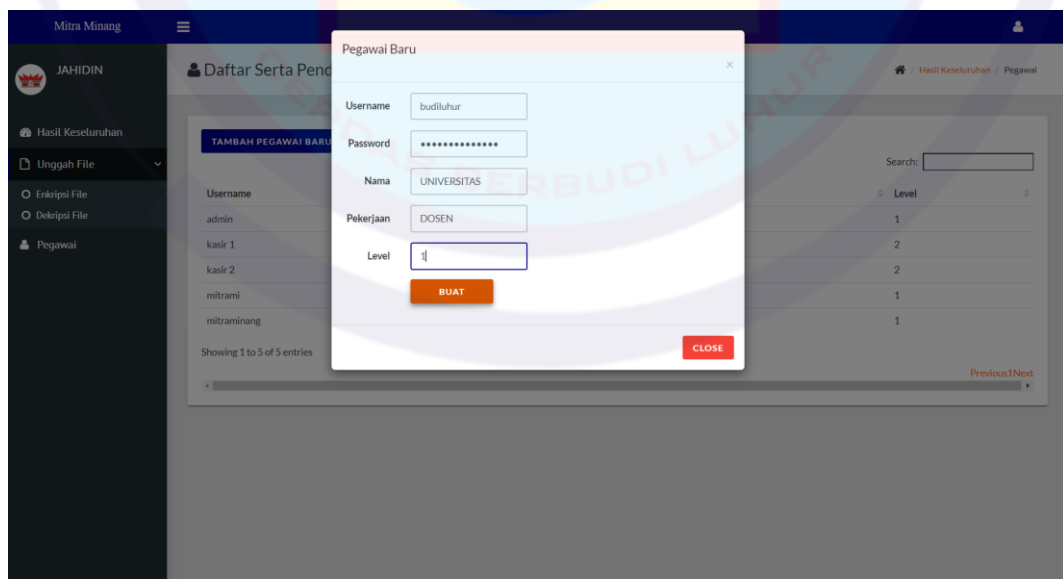
Pada tahap menu ini, bertujuan untuk melihat serta bisa untuk menambahkan pegawai baru, dengan cara mengklik menu “Tambah Pegawai Baru” Selanjutnya akan muncul *popup* untuk mengisi *Username*, *Password*, Nama, Pekerjaan, dan Status. Selanjutnya tinggal klik “BUAT”.

Berikut adalah menu halaman pegawai *admin* :



Gambar 4. 21 Menu halaman tambah pegawai *admin*

Berikut adalah menu halaman proses untuk tambah pegawai *admin* :



Gambar 4. 22 Menu halaman proses tambah pegawai

## **4.7 Evaluasi Program**

Setelah pengujian aplikasi ini selesai, ada beberapa keuntungan dan kekurangan, seperti berikut:

### **4.7.1 Kelebihan**

- a. Aplikasi ini dapat mengenkripsi *file word, PowerPoint, Excel*, PDF, serta jpg.
- b. Isi file tidak akan berubah setelah proses dekripsi selesai.
- c. Mudah dipahami dengan dan digunakan.

### **4.7.2 Kekurangan**

- a. Ukuran *file* yang ingin dienkripsi terbatas hanya 2 MB
- b. Tampilan masih kurang menarik



## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Setelah melakukan analisis dengan perancangan serta uji coba terhadap aplikasi enkripsi dan dekripsi, dengan Implementasi algoritma AES 128 berbasis web, maka disimpulkan sebagai berikut :

- a. Algoritma kriptografi *Advanced Encryption Standard* (AES) 128 telah berhasil di implementasikan pada aplikasi pengamanan data transaksi berbasis web pada Rumah Makan Mitra Minang.
- b. Aplikasi ini juga sudah diuji penuh untuk semua *file* dengan ekstensi docx, pdf, xlsx, pptx, dan jpg.
- c. Kecepatan waktu proses enkripsi dan dekripsi juga dipengaruhi oleh ukuran file semakin besar ukuran file, semakin lama waktu yang diperlukan untuk proses tersebut.

#### 5.2 Saran

Dalam hal ini ada pula saran untuk penelitian kali ini yang bertujuan untuk menambah peningkatan aplikasi keamanan enkripsi dan dekripsi.

- a. Diharapkan agar untuk ukuran *file* bisa ditingkatkan menjadi lebih besar dari sebelumnya.
- b. Diharapkan pada penelitian selanjutnya bisa menggunakan lebih dari satu algoritma.



## DAFTAR PUSTAKA

- Agustina, R. E., & Kurniati, A. (2009). *PEMANFAATAN KRIPTOGRAFI DALAM MEWUJUDKAN KEAMANAN INFORMASI PADA e-VOTING DI INDONESIA*.
- Hidayah, M. A., Budi Nugoho, N., & Iswan Perangin-Angin, M. (2020). Penerapan Kriptografi Menggunakan Algoritma AES untuk Keamanan Data Penjualan Pada PT.Mestika Sakti. *Jurnal CyberTech*, x. No.x.
- Hulu, D., Nadeak, B., & Aripin, S. (2020). *Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSUD Imelda Medan*. 4(1). <https://doi.org/10.30865/komik.v4i1.2590>
- May Sarah Sianturi, N., Budi Nugroho, N., & Rista Maya, W. (2020). Implementasi Kriptografi Untuk Pengamanan Data Aset Perusahaan Pada PT.PLN (Persero) Dengan Menggunakan Metode Algoritma AES 192. *Jurnal CyberTech*, x. No.x.
- Muharram, F., Azis, H., & Rachman, M. A. (2018). Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES). *Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi*, 3(2).
- Nandar Pabokory, F., Fitri Astuti, I., & Harsa Kridalaksana, A. (2015). IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD. In *Jurnal Informatika Mulawarman* (Vol. 10, Issue 1).
- Pramusinto, W., Wizaksono, N., & Saputro, A. (2019). Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman. *JURNAL BIT (Budi Luhur Information Technology)*, 16(2), 47–53.
- Pratiwi, & WP, A. D. (2016). *Peningkatan Keamanan Data dengan Metode Cropping Selection Pseudorandom*. <http://encoders-decoders.online-domain-tools.com>
- Pratomo, D., Budi Nugroho, N., & Ginting, R. I. (2019). IMPLEMENTASI KRIPTOGRAFI UNTUK MENGAMANKAN DATA PENJUALANAN DI PT. PAPPARICH MEDAN MENGGUNAKAN METODE AES 128. *Jurnal CyberTech*, x. No.x. <https://ojs.trigunadharma.ac.id/>
- Siringoringo, R. (2020). *Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File* (Vol. 02, Issue 01).
- Lyman, C. (2022). 5 jenis metode enkripsi (chiper) dalam kriptografi. <https://pintu.co.id/blog/jenis-enkripsi-cipher-kriptografi>

Oktavani, S et al., (2023). Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES). Siantar: Jumin.



## LAMPIRAN

### Lampiran 1 : SURAT KETERANGAN RISET

**Rumah Makan MITRA MINANG**

Jl. Ir. H. Juanda No.21 1, RT.14/RW.4, Kb. Klp., Kecamatan Gambir, Kota  
Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10120

WA / HP. 0882 - 1996 - 3906

---

**SURAT KETERANGAN RISET**

Yang bertanda tangan dibawah ini :

Nama : Jahidin  
Jabatan : Pemilik Rumah Makan Mitra Minang


Menerangkan bahwa :

Nama : Ilham Wahyu Kuncoro Aji  
NIM : 1911510798

Telah melaksanakan riset pada Usaha Mikro, kecil, dan Menengah (UMKM),  
yaitu Rumah Makan Mitra Minang sejak tanggal 3 Mei 2024 sampai dengan 13  
Juni 2024 dengan baik.

Demikian Surat Keterangan ini dibuat untuk dapat dipergunakan semestinya.

Dibuat di : Jakarta  
Kamis. 13 Juli 2024

  
Jahidin  
**CIPTA MINANG**  
(Pemilik Rumah Makan Mitra Minang)  
Jl. Ir. H. Juanda 21 B Jakarta Pusat | Samping Sinarum Teyala |  
☎ 0882 1996 3906 📠 (021) 3840137

Lampiran 2 : Hasil Cek *Similarity*

ilham-turnitin1			
ORIGINALITY REPORT			
11%	%	%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS
PRIMARY SOURCES			
1	Submitted to Universitas Budi Luhur Student Paper	8%	
2	Submitted to Universitas Esa Unggul Student Paper	1%	
3	Submitted to Universitas Muria Kudus Student Paper	1%	
4	Submitted to Universitas Papua Student Paper	1%	
Exclude quotes On			
Exclude bibliography On			
Exclude matches < 1%			