

## Penerapan Algoritma Kriptografi *Advanced Encryption Standard* 128 Pada Laporan Transaksi Di Kopi Tuku

Mufti<sup>1</sup>, Yudi Wiharto<sup>2</sup>, Subandi<sup>3</sup>

<sup>1,2</sup>Jurusan Teknik Informatika, Universitas Budi Luhur, Indonesia

<sup>3</sup>Jurusan Sistem Informasi, Universitas Budi Luhur, Indonesia

<sup>1</sup>[mufti@budiluhur.ac.id](mailto:mufti@budiluhur.ac.id), <sup>2</sup>[yudi.wiharto@budiluhur.ac.id](mailto:yudi.wiharto@budiluhur.ac.id), <sup>3</sup>[subandi.spd@budiluhur.ac.id](mailto:subandi.spd@budiluhur.ac.id)

### Informasi Artikel

#### Article historys:

Submit Okt 24, 2024

Review 1 Des 4, 2024

Review 2 Des 28, 2024

Publish Jan 30, 2025

#### Kata Kunci:

AES 128-bit;  
Cryptography;  
Data Security;  
Encryption;  
Kopi Tuku;

### ABSTRACT

Data security is an important aspect in information management, especially in business transactions involving sensitive data such as financial reports. This study aims to apply the *Advanced Encryption Standard* (AES) 128-bit cryptographic algorithm to transaction report data at Kopi Tuku. AES 128-bit was chosen because of its ability to provide strong and efficient data encryption, with a high level of security and adequate processing speed. In this study, transaction data was taken from the Kopi Tuku sales system and encrypted using AES 128-bit to protect sensitive information from unauthorized access. The encryption and decryption processes were tested to ensure data integrity and security. The results showed that the implementation of AES 128-bit successfully maintained the confidentiality and security of transaction data without reducing system performance. This study concludes that the AES 128-bit algorithm is an effective solution to improve transaction data security in the coffee industry, especially in small and medium-sized businesses such as Kopi Tuku.

#### \*Koresponden Author:

Yudi Wiharto,  
Jurusan Teknik Informatika,  
Universitas Budi Luhur,  
Jl. Ciledug Raya, Petukangan Utara, Kota Jakarta Selatan, Indonesia.  
Email: [yudi.wiharto@budiluhur.ac.id](mailto:yudi.wiharto@budiluhur.ac.id)



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

### 1. PENDAHULUAN

Di era digital yang semakin berkembang pesat, kebutuhan akan keamanan data menjadi salah satu prioritas utama dalam berbagai sektor, termasuk bisnis. Perkembangan teknologi informasi yang sangat pesat turut memajukan media komunikasi sebagai media penyampaian informasi dari satu tempat ke tempat lain, sehingga memudahkan orang dalam mengakses media komunikasi, Kemudahan pengaksesan media komunikasi oleh semua orang, membuat informasi menjadi aspek sangat rentan untuk diketahui, diambil dan dimanipulasi oleh pihak – pihak yang tidak bertanggung jawab [1]. Transaksi digital yang melibatkan data sensitif, seperti laporan keuangan dan informasi pelanggan, memerlukan sistem keamanan yang andal untuk mencegah kebocoran data atau akses tidak sah. Keamanan data tidak hanya penting untuk menjaga privasi, tetapi juga untuk melindungi integritas bisnis dan kepercayaan pelanggan.

Kopi Tuku, sebagai salah satu usaha kopi lokal yang berkembang pesat, juga menghadapi tantangan serupa. Dengan meningkatnya volume transaksi harian, kebutuhan akan perlindungan data transaksi menjadi semakin mendesak. Dalam hal ini, teknologi kriptografi berperan penting sebagai solusi yang dapat diandalkan untuk mengamankan data sensitif. Kriptografi modern menyediakan berbagai algoritma enkripsi yang dirancang untuk melindungi data dari ancaman eksternal. Salah satu algoritma kriptografi yang banyak digunakan dalam berbagai aplikasi keamanan data adalah *Advanced Encryption Standard* (AES). AES memiliki keunggulan yaitu dapat digunakan untuk penyandian dengan melakukan enkripsi perblok (128 bit) secara paralel untuk memudahkan proses enkripsi maupun dekripsi [2]. Data-data yang bersifat personal tidak sepatutnya diketahui oleh orang lain untuk menekan terjadinya data tersebut disalahgunakan dan dimanfaatkan tanpa izin pengguna selaku yang berhak atas data-data tersebut [3]. Kriptografi adalah bidang ilmiah yang mempelajari teknologi enkripsi data, kriptografi dibagi menjadi dua jenis, klasik dan modern, dengan kunci simetris dan asimetris [4]. AES merupakan algoritma simetris yang terkenal karena efisiensinya dalam proses enkripsi dan dekripsi, serta tingkat keamanan yang tinggi. Cara yang bisa digunakan untuk mengamankan data dan informasi adalah enkripsi, dimana enkripsi dilakukan pada saat penyimpanan ke dalam basis data, sedangkan dekripsi proses perubahan data dari bentuk acak jadi data asli, data aslinya bisa dilihat dengan menggunakan kunci rahasia yang telah diberikan [5]. Algoritma ini memiliki beberapa varian berdasarkan panjang kunci yang digunakan, yaitu AES 128-bit, 192-bit, dan 256-bit. Untuk penerapan di Kopi Tuku, AES 128-bit dipilih karena keseimbangan antara keamanan yang kuat dan kecepatan pemrosesan yang cocok untuk usaha kecil dan menengah.

Penelitian ini bertujuan untuk menerapkan algoritma kriptografi AES 128-bit pada data laporan transaksi di Kopi Tuku. Melalui penerapan ini, diharapkan data transaksi dapat terenkripsi dengan baik sehingga terhindar dari risiko akses tidak sah dan manipulasi data. Untuk menjaga agar data yang tersimpan diblokir untuk pihak yang tidak disetujui maka diperlukan pengamanan data [6]. Penelitian ini juga akan mengevaluasi kinerja enkripsi dan dekripsi AES 128-bit pada sistem laporan transaksi di Kopi Tuku untuk memastikan bahwa implementasi tersebut tidak mengganggu operasi sistem yang ada. pengamanan file yang dilakukan dengan cara enkripsi sehingga hanya orang yang mengetahui kunci yang dapat mendekripsi file agar file tersebut dapat kembali seperti semula dan file tidak dapat dipahami oleh pihak yang tidak berhak atau yang tidak memiliki kunci [7]. Melalui penelitian ini, diharapkan solusi enkripsi berbasis AES 128-bit dapat meningkatkan tingkat keamanan data transaksi tanpa mengurangi efisiensi operasional Kopi Tuku. Dengan menerapkan teknologi enkripsi seperti *Advanced Encryption Standard* (AES), memastikan bahwa setiap data terjaga kerahasiaannya dan tidak dapat diakses oleh pihak yang tidak berwenang [8]. Tujuan utama adalah meningkatkan keamanan data pengguna pada sistem dan menyediakan solusi yang efektif untuk melindungi informasi sensitif [9].

## 2. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif untuk menerapkan dan menguji efektivitas algoritma kriptografi *Advanced Encryption Standard* (AES) 128-bit dalam pengamanan data laporan transaksi di Kopi Tuku. Dengan penerapan Algoritma AES 128, aplikasi ini dapat menjaga kerahasiaan dan integritas data bansos, mencegah kebocoran informasi, dan melindungi data dari pencurian [10]. Adapun tahapan-tahapan yang dilakukan dalam penelitian ini meliputi:

### 1. Pengumpulan Data

Data yang digunakan dalam penelitian ini adalah data transaksi harian dari sistem penjualan Kopi Tuku, yang mencakup informasi seperti tanggal transaksi, jumlah transaksi, produk

yang dijual, serta rincian pelanggan. Data ini diambil dari database penjualan yang sudah berjalan untuk dilakukan proses enkripsi.

## 2. Desain Sistem Enkripsi

Pada tahap ini, sistem enkripsi dirancang menggunakan algoritma AES 128-bit. Desain ini mencakup pemilihan metode enkripsi simetris, di mana kunci enkripsi dan dekripsi yang digunakan adalah sama. Proses enkripsi dilakukan terhadap data laporan transaksi, sehingga hanya pihak yang memiliki kunci yang benar dapat melakukan dekripsi dan mengakses informasi asli.

## 3. Langkah-langkah desain meliputi:

1. Pemilihan bahasa pemrograman dan library kriptografi yang mendukung algoritma AES 128-bit.
2. Implementasi proses enkripsi terhadap data transaksi menggunakan kunci enkripsi yang telah ditentukan.
3. Implementasi proses dekripsi untuk memastikan data yang dienkripsi dapat dikembalikan ke bentuk semula tanpa kehilangan informasi.

## 4. Implementasi Enkripsi

Pada tahap ini, algoritma AES 128-bit diimplementasikan pada data laporan transaksi. langkah ini meliputi proses:

1. Enkripsi: Data transaksi yang diambil dari sistem penjualan dienkripsi menggunakan algoritma AES 128-bit
2. Penyimpanan data terenkripsi: Data yang telah dienkripsi kemudian disimpan di dalam database baru untuk tujuan keamanan.
3. Dekripsi: Data yang telah dienkripsi diuji dengan proses dekripsi menggunakan kunci yang sama untuk memastikan bahwa data dapat diakses kembali dengan benar.

## 5. Pengujian Kinerja

Setelah implementasi algoritma AES 128-bit, dilakukan pengujian kinerja sistem untuk mengevaluasi seberapa efektif algoritma ini dalam menjaga keamanan data tanpa mengurangi kinerja sistem. Pengujian dilakukan dengan beberapa indikator, seperti mengukur seberapa cepat proses enkripsi dan dekripsi dilakukan pada dataset laporan transaksi yang besar. Memastikan bahwa data transaksi setelah dekripsi sesuai dengan data asli sebelum dienkripsi, untuk menjaga keakuratan informasi.

## 6. Analisis Data

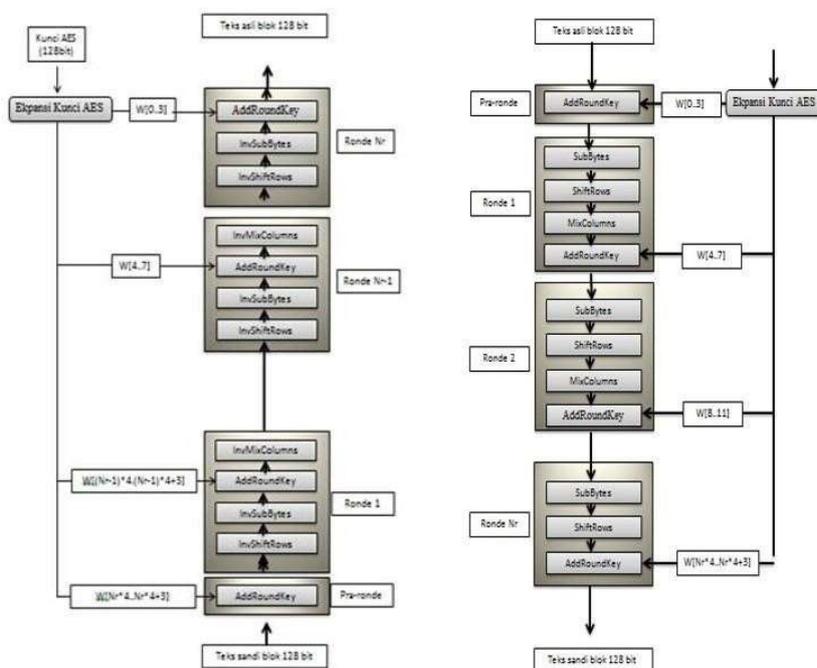
Data hasil pengujian kinerja dianalisis secara kuantitatif untuk menilai efektivitas penerapan algoritma AES 128-bit. Analisis ini mencakup perbandingan waktu pemrosesan enkripsi-dekripsi, efisiensi penyimpanan data terenkripsi, serta evaluasi keamanan data. Hasil pengujian kemudian digunakan untuk menarik kesimpulan tentang kesesuaian algoritma AES 128-bit dalam konteks keamanan data di Kopi Tuku.

## 7. Kesimpulan

Berdasarkan hasil implementasi dan pengujian, penelitian ini akan menarik kesimpulan tentang efektivitas penerapan algoritma AES 128-bit dalam mengamankan data laporan transaksi di Kopi Tuku. Kesimpulan ini juga akan mencakup rekomendasi untuk

implementasi lebih lanjut, seperti optimalisasi sistem atau penggunaan varian algoritma enkripsi lain jika diperlukan.

Dengan metode ini, diharapkan penerapan algoritma AES 128-bit pada Kopi Tuku dapat berjalan optimal dan memberikan perlindungan yang memadai terhadap data transaksi. Pemakaian metode *Advanced Encryption Standard* (AES) ini dapat mengamankan data dengan tingkat keamanan yang tinggi [11].



Gambar 1. Proses enkripsi dan dekripsi

Algoritma kriptografi *Advanced Encryption Standard* (AES) 128-bit yang diterapkan dalam penelitian ini bertujuan untuk mengamankan data laporan transaksi di Kopi Tuku. Berikut adalah perumusan algoritma untuk proses enkripsi dan dekripsi menggunakan AES 128-bit.

1. Langkah-langkah Enkripsi Data Menggunakan AES 128-bit

1. Input:
  - a. Plaintext (data transaksi): Data laporan transaksi yang akan dienkripsi.
  - b. Kunci (key): Kunci enkripsi sepanjang 128-bit (16 byte).
2. Output:
 

Ciphertext: Data transaksi yang telah terenkripsi.
3. Algoritma:
  1. Pembangkitan Kunci
 

Buat kunci enkripsi simetris dengan panjang 128-bit (16 byte). Kunci ini akan digunakan untuk proses enkripsi dan dekripsi.
  2. Pembagian Plaintext
 

Jika panjang data (plaintext) lebih besar dari blok standar AES (16 byte), bagi plaintext menjadi blok-blok berukuran 128-bit. Jika panjang data kurang dari 16 byte, tambahkan padding sesuai standar PKCS#7 agar panjangnya genap 16 byte.
  3. SubByte

Lakukan substitusi byte pada setiap blok menggunakan tabel substitusi (S-box) untuk meningkatkan difusi. Setiap byte di plaintext diganti dengan byte yang sesuai dari S-box.

4. ShiftRow

Lakukan rotasi byte pada setiap baris dalam blok data. Setiap baris dari blok di-shift ke kiri dengan jumlah tertentu: baris pertama tidak di-shift, baris kedua di-shift 1 byte, baris ketiga di-shift 2 byte, dan baris keempat di-shift 3 byte.

5. MixColumn

Lakukan transformasi linear pada setiap kolom data untuk meningkatkan difusi. Setiap kolom dikalikan dengan matriks tetap yang telah ditentukan.

6. AddRoundKey

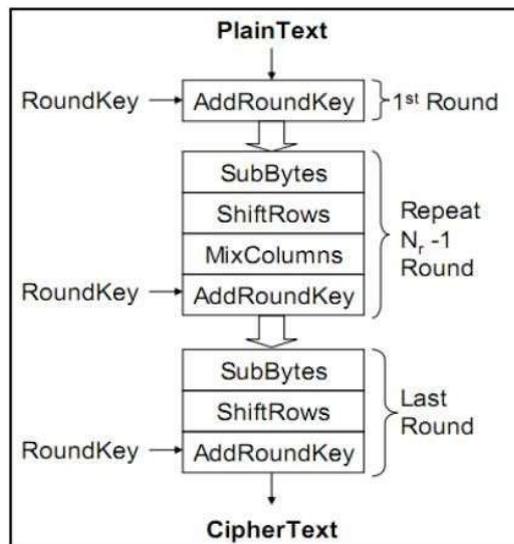
XOR setiap blok data dengan kunci round yang dihasilkan dari proses pembangkitan kunci.

7. Ulangi Proses untuk 9 Ronde Selanjutnya

Langkah 3 hingga 6 diulang sebanyak 9 kali. Pada ronde ke-10, proses MixColumn tidak dilakukan untuk menjaga efisiensi.

8. Hasil Akhir Enkripsi

Setelah semua ronde selesai, hasil akhirnya adalah ciphertext, yaitu data transaksi yang telah dienkripsi.



Gambar 2. Proses Enkripsi

2. Langkah-langkah Dekripsi Data Menggunakan AES 128-bit

1. Input:

Ciphertext: Data transaksi yang telah terenkripsi.

Kunci (key): Kunci dekripsi (sama dengan kunci enkripsi 128-bit).

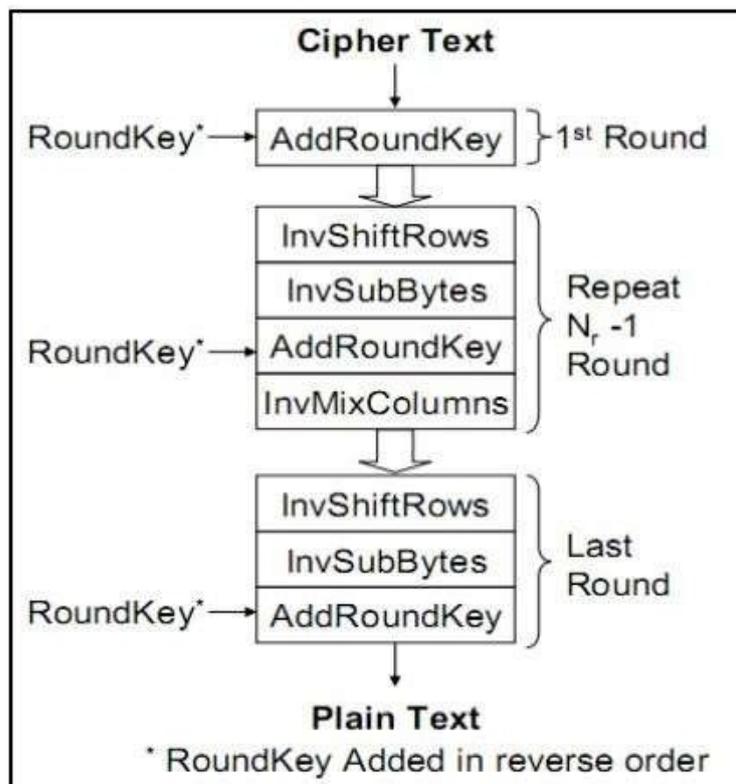
2. Output:

Plaintext: Data transaksi asli setelah didekripsi.

3. Algoritma:

1. Pembagian Ciphertext

- Bagi ciphertext menjadi blok-blok 128-bit. Jika terdapat padding, catat untuk menghapusnya setelah dekripsi.
2. AddRoundKey (Ronde Ke-10)  
Lakukan XOR antara blok ciphertext dan kunci round terakhir (kunci ronde ke-10 dari pembangkitan kunci).
  3. Inverse ShiftRow  
Lakukan proses inverse dari ShiftRow pada setiap blok: rotasi byte ke kanan untuk setiap baris (baris pertama tetap, baris kedua di-shift 1 byte ke kanan, dan seterusnya).
  4. Inverse SubByte  
Ganti byte di setiap blok dengan nilai inversnya dari tabel S-box (menggunakan inverse S-box).
  5. Inverse MixColumn (Hanya untuk Ronde 1 hingga 9)  
Lakukan inverse dari MixColumn untuk mengembalikan data ke bentuk semula.
  6. AddRoundKey (Ronde Sebelumnya)  
XOR setiap blok dengan kunci round yang sesuai. Ulangi proses dari ronde 9 hingga ronde 1.
  7. Hasil Dekripsi  
Setelah semua ronde selesai, gabungkan blok-blok data untuk mendapatkan plaintext asli. Jika ada padding, hapus padding sesuai aturan yang digunakan.

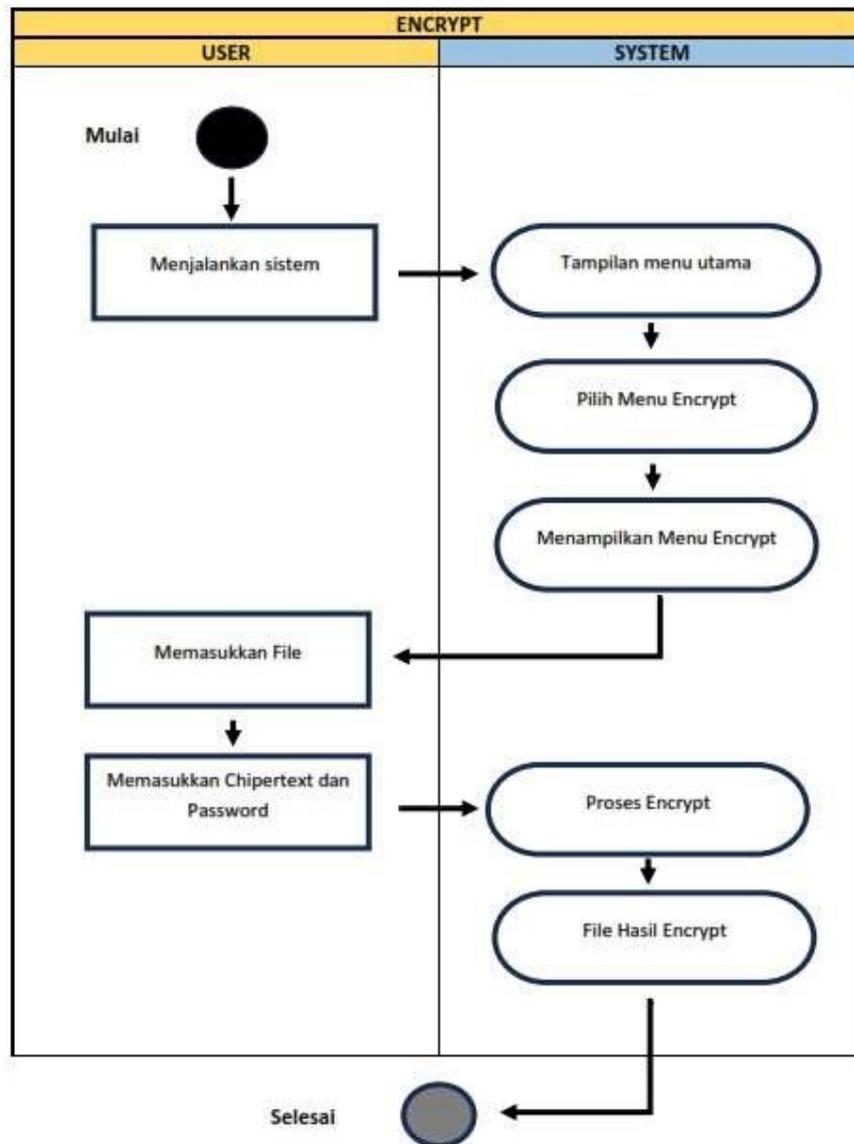


Gambar 3. Proses Dekripsi

### 3. HASIL PENELITIAN DAN PEMBAHASAN

#### 3.1. Analisis Sistem Yang Berjalan

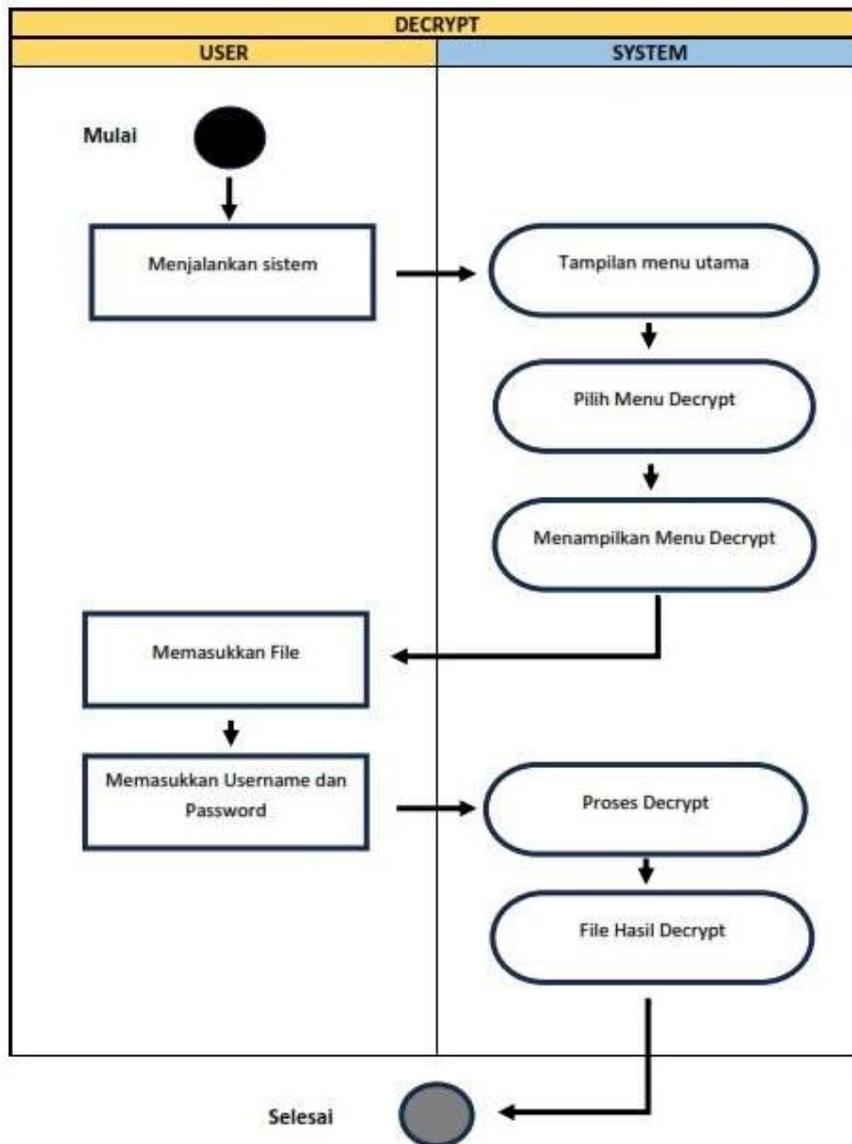
##### a. Activity Diagram Encrypt



Gambar 4. Activity Diagram Encrypt

Aktivitas ini, diawali dengan membuka aplikasi kemudian ditampilkan Menu utama, setelah itu pada proses enkripsi pengguna kemudian memilih menu encrypt dan masuk ke form encrypt lalu mengupload file yang akan dienkripsi dengan memberikan password dilanjutkan dengan proses enkripsi setelah proses selesai maka file hasil enkripsi dapat langsung didownload.

b. Activity Diagram Decrypt



Gambar 5. Activity Diagram Decrypt

Pada aktivitas ini, dimulai dengan tampilan menu utama, setelah itu pengguna kemudian memilih menu decrypt dan masuk lalu mengupload file hasil enkripsi yang akan didekripsi dengan memberikan password dilanjutkan dengan proses dekripsi setelah proses selesai maka file hasil dekripsi dapat langsung didownload.

### 3.2. Algoritma

Algoritma adalah serangkaian langkah atau instruksi logis yang dirancang untuk menyelesaikan suatu permasalahan atau tugas tertentu. Pada bagian ini, akan dibahas hasil dari penerapan algoritma kriptografi *Advanced Encryption Standard* (AES) 128-bit pada data laporan transaksi di Kopi Tuku. Berikut ini adalah algoritma proses enkripsi dan dekripsi.

a. *Algoritma proses Enkripsi*

1. Proses Encrypt
2. Inisialisasi Algoritma = AES-128
3. Inisialisasi IV (Initialization Vector) = 10tomadj+26h21r790
4. Inisialisasi Error = 0
5. Check Password
6. Check File
7. If Password == salah Then : Status = Invalid Password
8. If File == Tidak Didukung Then : Status = Error
9. Mengambil dan Membaca File.
10. Enkripsi data menggunakan openssl\_encrypt dengan algoritma, password, iv
11. Mengubah ekstensi file menjadi .hidden
12. Mengirim file untuk diunduh secara otomatis ke user

b. *Algoritma proses Dekripsi*

1. Proses Decrypt
2. Inisialisasi Algoritma = AES-128
3. Inisialisasi IV (Initialization Vector) = 10tomadj+26h21r790
4. Inisialisasi Error = 0
5. Check Password
6. Check File
7. If Password == salah Then : Status = Invalid Password
8. If File == Tidak Didukung Then : Status = Error
9. Mengambil dan Membaca File.
10. Dekripsi data menggunakan openssl\_decrypt dengan algoritma, password, iv
11. Mengubah ekstensi file menjadi .hidden
12. Mengirim file untuk diunduh secara otomatis ke user

**3.3. Implementasi**

Pengujian menu enkripsi dilakukan dengan bertujuan untuk mengetahui sistem apakah berjalan baik dan sesuai yang diprediksi. Pengujian ini di lakukan dengan menggunakan file sampel dan melakukan cek apakah fungsional dari menu enkripsi yang dibuat bekerja dengan sesuai.

**Table 1.** Skenario pengujian enkripsi

No	Fitur/Menu Yang Di Uji	Skenario	Pengujian
1	Enkripsi	<input type="checkbox"/> Memasukan File berjenis Docx, Doc, Txt, Pdf, Xls, Xlsx, Ppt, Pptx <input type="checkbox"/> Memasukan kunci	Fungsional

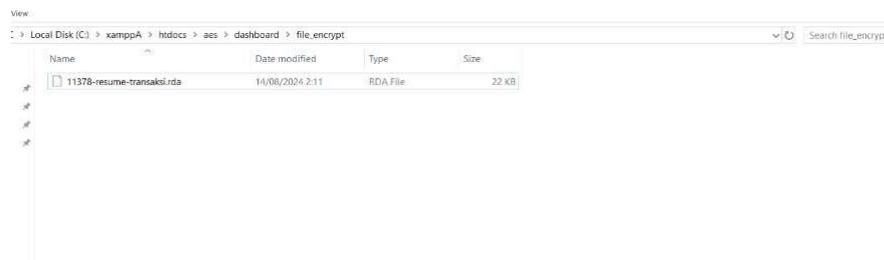
Table diatas adalah proses skenario dari pengujian enkripsi dengan file sampel yang akan di ujikan, beberapa contoh sampel file dengan ekstensi doc, docx, txt, pdf, xls, xlsx, ppt, pptx.

Table 2. Skenario pengujian deskripsi

No	Fitur/Menu Yang Di Uji	Skenario	Pengujian
1	Dekripsi	<ul style="list-style-type: none"> <li><input type="checkbox"/> Pilih Opsi Dekripsi pada berkas yang akan didekripsi</li> <li><input type="checkbox"/> Memasukan kunci</li> </ul>	Fungsional

Table diatas adalah proses skenario dari pengujian dekripsi dengan file hasil enkripsi yang akan di ujikan.

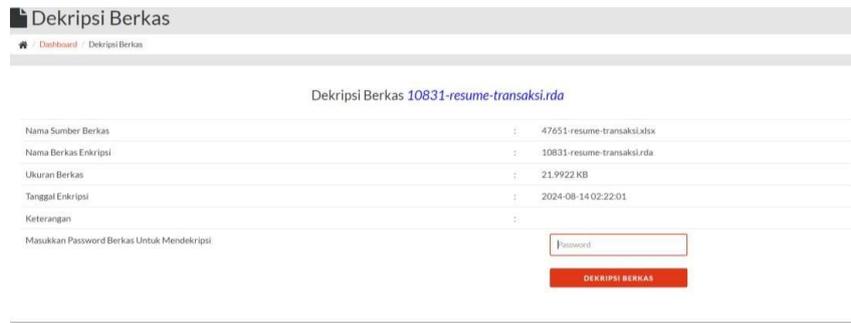
Gambar 6. Menu Enkripsi



Gambar 7. File hasil enkripsi

No	Nama Sumber Berkas	Nama Berkas Enkripsi	Path Berkas	Status Berkas	Opsi
1	94843-resume-transaksi.xlsx	50047-resume-transaksi.rda	file_encrypt/50047-resume-transaksi.rda	Dekripsi	<div style="background-color: green; color: white; padding: 2px;">ENKRIPSI BERKAS</div> <div style="background-color: red; color: white; padding: 2px;">HAPUS BERKAS</div>

Gambar 8. Menu Dekripsi

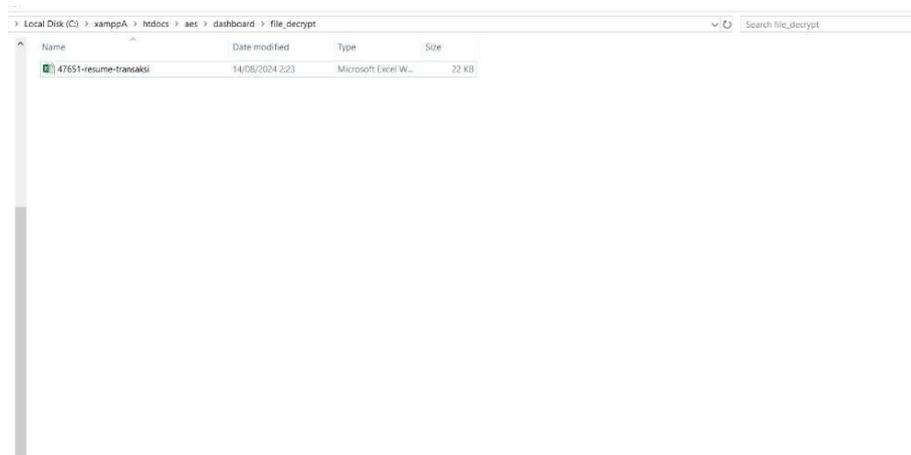


**Gambar 9.** Proses Dekripsi File

Setelah dilakukan proses dekripsi, data yang dihasilkan 100% sesuai dengan data asli. Tidak ada perubahan atau kerusakan pada informasi, menunjukkan bahwa algoritma AES 128-bit mampu menjaga integritas data dengan sangat baik.

**Table 3.** Hasil pengujian

No	Nama File dan Tipe	Password	Ukuran file (kb)	Waktu Enkripsi (detik)	Waktu Dekripsi (Detik)
1	laporan transaksi.pdf	admin	281	23.5	23.6
2	laporan transaksi.doc	admin	57	6.3	6.7
3	laporan transaksi.xls	admin	22kb	14.3	14.6



**Gambar 10.** Hasil dekripsi

Dari hasil ini, dapat disimpulkan bahwa AES 128-bit mampu mengenkripsi dan mendekripsi data laporan transaksi dengan kecepatan yang masih dapat diterima tanpa mengurangi kinerja sistem secara signifikan. Pemrosesan yang cepat ini penting agar sistem penjualan Kopi Tuku tetap berfungsi dengan lancar tanpa ada hambatan yang berarti. Penerapan AES 128-bit pada sistem laporan transaksi di Kopi Tuku terbukti berjalan dengan baik. Sistem mampu mengenkripsi dan mendekripsi data transaksi dalam waktu yang wajar tanpa mengganggu kinerja operasional sehari-

hari. Selain itu, AES 128-bit mampu melindungi data transaksi dari ancaman akses tidak sah, sehingga meningkatkan keamanan dan kepercayaan terhadap sistem penjualan Kopi Tuku.

Dalam konteks usaha kecil dan menengah seperti Kopi Tuku, penerapan AES 128-bit sangat sesuai karena menawarkan keseimbangan antara keamanan yang kuat, kinerja yang cepat, dan efisiensi penyimpanan. Oleh karena itu, algoritma ini direkomendasikan untuk digunakan secara luas dalam pengamanan data transaksi yang sensitif.

#### 4. KESIMPULAN

Kesimpulan dari penelitian ini adalah bahwa penerapan algoritma kriptografi *Advanced Encryption Standard* (AES) 128-bit pada data laporan transaksi di Kopi Tuku berhasil meningkatkan keamanan data dengan efisien tanpa mengganggu kinerja sistem. Algoritma AES 128-bit mampu mengenkripsi dan mendekripsi data transaksi dengan cepat, menjaga integritas informasi, serta melindungi data dari potensi akses tidak sah. Selain itu, algoritma ini terbukti cocok digunakan dalam lingkungan usaha kecil dan menengah seperti Kopi Tuku, karena memberikan keseimbangan antara keamanan, efisiensi waktu pemrosesan, dan kapasitas penyimpanan.

#### DAFTAR PUSTAKA

- [1] T. Bin Tahir, M. A. Hs, M. Rais, and I. Syarif, "Sistem Informasi Encrypt Dan Decrypt Dengan Algoritma AES Menggunakan Framework Laravel," *PATRIA ARTHA Technological Journal* •, vol. 4, no. 1, pp. 41–46, Apr. 2020, Accessed: Oct. 21, 2024. [Online]. Available: <https://www.ejournal.patria-artha.ac.id/index.php/patj/article/download/326/269>
- [2] H. Wijaya, "JURNAL AKADEMIKA PENERBIT IMPLEMENTASI KRIPTOGRAFI AES-128 UNTUK MENGAMANKAN URL (UNIFORM RESOURCE LOCATOR) DARI SQL INJECTION," *JURNAL AKADEMIKA*, vol. 17, no. 1, pp. 8–13, Jan. 2020, Accessed: Oct. 21, 2024. [Online]. Available: <blob:https://ejournal.lppmunidayan.ac.id/fde4ff20-0fd8-4072-823b-234fa3f441de>
- [3] L. Clara and A. Budi, "IMPLEMENTASI METODE ALGORITMA AES PADA PERLINDUNGAN DATA SISTEM LOGIN," *Jurnal Informatika Dan Bisnis*, vol. 10, no. 2, pp. 1–14, Dec. 2021, Accessed: Oct. 21, 2024. [Online]. Available: <https://jurnal.kwikkiangie.ac.id/index.php/JIB/article/download/791/523/2553>
- [4] M. Azhari, J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi *Advanced Encryption Standard* (AES)," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 163–171, Mar. 2022, doi: 10.47709/jpsk.v2i1.1390.
- [5] Y. Wiharto and Mufti, "Implementasi *Advanced Encryption Standard* 128 Sebagai Pengamanan Basis Data Obat-obatan Apotek," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 2, pp. 335–350, Aug. 2022, doi: 10.28932/jutisi.v8i2.4817.
- [6] B. Olivia Putri Irine Irawan, M. Tahir, N. Ayu Windrastuti, D. Yurina Cholili, D. Mulaikah, and A. Batsul Mushofi Septian wachid, "IMPLEMENTASI KRIPTOGRAFI PADA KEAMANAN DATA MENGGUNAKAN ALGORITMA ADVANCE ENCRYPTION STANDARD (AES)," *Jurnal SimanteC*, vol. 11, no. 2, pp. 167–174, Jun. 2023, Accessed: Oct. 21, 2024. [Online]. Available: <https://journal.trunojoyo.ac.id/simantec/article/download/20034/8432>
- [7] I. Priambudi and Mufti, "Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 6, no. 1, pp. 22–31, Jan. 2023, Accessed: Oct. 21, 2024. [Online]. Available: <blob:https://jom.fti.budiluhur.ac.id/18f1e1a0-8387-48dc-bc53-b00ef53cc39f>
- [8] Khusaeri Andesa, Afhand Fachzevi, Torkis Nasution, and Herwin, "Implementasi Metode AES pada Aplikasi Chat Menggunakan Flutter," *SATIN - Sains dan Teknologi Informasi*, vol. 9, no. 2, pp. 216–226, Dec. 2023, doi: 10.33372/stn.v9i2.1075.
- [9] N. F. Aprilia, D. Mafa, A. R. Muchtar, K. A. A. Rohim, and R. N. I. Firdaus, "Penerapan Algoritma AES untuk Enkripsi pada Halaman Register serta Penerapan AES untuk Deskripsi pada Halaman Login Website," *Journal of Informatics Development*, vol. 1, no. 2, pp. 75–82, Apr. 2023, doi: 10.30741/jid.v1i2.1041.
- [10] Y. Agita, P. Tarigan, R. Aulia, and A. M. Elhanafi, "Algoritma AES 128 dalam Mengenkripsikan Berkas Bansos Kecamatan Tigabinanga Berbasis Web," *Jurnal Unitek*, vol. 17, no. 2, pp. 193–204,

- Dec. 2024, Accessed: Oct. 21, 2024. [Online]. Available:  
<https://ejurnal.sttdumai.ac.id/index.php/unitek/article/download/943/493/4880>
- [11] A. Sura Pratama and Sriyanto, "IMPLEMENTASI KEAMANAN DATA NILAI SISWA MENGGUNAKAN METODE *ADVANCED ENCRYPTION STANDARD* (AES) (Studi Kasus : Sekolah Menengah Pertama Negeri (SMPN) 3 Bungku)," *Jurnal IndraTech*, vol. 5, no. 1, pp. 60–73, May 2024, Accessed: Oct. 21, 2024. [Online]. Available:  
<https://ojs.stmikindragiri.ac.id/index.php/jit/article/download/140/139>