

# IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 UNTUK MENGAMANKAN DATA PENJUALAN DI TOKO DIAH KEMASAN KOSMETIK

Danang Pandya Pangestu<sup>1\*</sup>, Dolly Virgianshaka Yudha Sakti<sup>2</sup>

<sup>1,2</sup>Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: <sup>1\*</sup>2111530065@student.budiluhur.ac.id, <sup>2</sup>dolly.virgianshaka@budiluhur.ac.id

**Abstrak**-Pesatnya perkembangan teknologi informasi mempermudah pengelolaan data penjualan pada sektor UMKM, namun juga meningkatkan potensi risiko kebocoran dan manipulasi data. Penelitian ini bertujuan mengimplementasikan algoritma kriptografi *Advanced Encryption Standard* (AES) 128-bit modifikasi guna meningkatkan keamanan data penjualan di Toko Diah Kemasan Kosmetik. Metode yang digunakan adalah pendekatan implementasi melalui perancangan aplikasi berbasis *web* yang mampu melakukan enkripsi dan dekripsi *file* data penjualan, dengan pengujian fungsional menggunakan metode *black box*. Hasil penelitian menunjukkan bahwa dengan memodifikasi *round* enkripsi dan dekripsi AES-128 mampu menjaga kerahasiaan dan integritas data secara efektif dengan kinerja pemrosesan yang efisien, meskipun masih terdapat keterbatasan pada manajemen kunci dan ketiadaan fitur pemulihan data. Kesimpulannya, implementasi AES-128 modifikasi dapat menjadi solusi praktis untuk peningkatan keamanan informasi pada UMKM serta menjadi dasar pengembangan sistem keamanan data yang lebih komprehensif di masa mendatang.

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

## ***IMPLEMENTATION OF THE AES-128 CRYPTOGRAPHIC ALGORITHM FOR SECURING SALES DATA AT TOKO DIAH KEMASAN KOSMETIK***

**Abstract**-The rapid advancement of information technology facilitates sales data management in Micro, Small, and Medium Enterprises (MSMEs) while increasing the risk of data breaches and manipulation. This study aims to implement a modified Advanced Encryption Standard (AES) 128-bit cryptographic algorithm to enhance sales data security at Toko Diah Kemasan Kosmetik. The research employed an implementation approach through the design of a web-based application capable of encrypting and decrypting sales data files, with functional testing conducted using the black box method. The research results show that by modifying the encryption and decryption rounds in AES 128 effectively maintains data confidentiality and integrity with efficient processing performance, although limitations remain in key management and the absence of a data recovery feature. In conclusion, the modified AES-128 implementation offers a practical solution for improving information security in MSMEs and serves as a foundation for the development of more comprehensive data protection systems in the future.

**Keywords:** *Cryptography, AES-128, Data Security, Encryption, Decryption.*

---

## 1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam operasional bisnis, khususnya pada pencatatan dan pengelolaan data penjualan. Digitalisasi sistem informasi penjualan memberikan keuntungan dari segi kecepatan, efisiensi, dan akurasi, namun juga memunculkan risiko seperti kebocoran data, modifikasi tanpa otorisasi, serta penyalahgunaan informasi pelanggan [1]. Risiko ini sangat relevan bagi pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) yang sering mengadopsi sistem digital tanpa dilengkapi mekanisme keamanan yang memadai.

Toko Diah Kemasan Kosmetik, sebagai salah satu pelaku UMKM di bidang penjualan kemasan kosmetik, telah menerapkan sistem digital dalam pengelolaan data penjualan, tetapi belum memiliki fitur keamanan yang

optimal untuk menjamin kerahasiaan dan integritas data transaksi. Mengingat data penjualan merupakan aset vital, dibutuhkan langkah strategis untuk melindungi informasi tersebut dari ancaman keamanan.

Kriptografi merupakan teknologi utama yang digunakan untuk menjaga keamanan data. Di antara berbagai algoritma yang ada, *Advanced Encryption Standard* (AES) telah banyak diadopsi karena tingkat keamanan yang tinggi dan efisiensi komputasinya [2][3]. AES adalah algoritma simetris berbasis blok yang mendukung panjang kunci 128, 192, dan 256 bit, sehingga data yang terenkripsi hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang benar. Berbagai penelitian telah menunjukkan keberhasilan penerapan AES di berbagai bidang, seperti pengamanan data penjualan [4][5], perlindungan dokumen keuangan [6], pengamanan basis data pasien [7], transaksi *e-marketplace* [8], keamanan data penjualan otomotif [9], serta enkripsi dokumen pada instansi pemerintah [10].

Dikarenakan belum ada penerapan pada UMKM kemasan kosmetik dengan fokus pada pengamanan *file* penjualan, dan penelitian ini dibuat menggunakan metode AES-128 dengan memodifikasi round enkripsi dan dekripsinya agar lebih efisiensi untuk UMKM dengan keterbatasan sumber daya seperti Toko Diah Kemasan Kosmetik.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada penerapan algoritma AES-128 untuk mengamankan data penjualan pada sistem informasi yang digunakan di Toko Diah Kemasan Kosmetik. Penelitian ini bertujuan untuk merancang dan mengimplementasikan proses enkripsi dan dekripsi data penjualan menggunakan AES-128, serta mengevaluasi efektivitasnya dalam menjaga kerahasiaan dan integritas data. Secara ilmiah, penelitian ini berkontribusi pada literatur terkait penerapan kriptografi di sektor ritel kosmetik yang masih minim kajian akademis. Hasil penelitian diharapkan dapat memberikan solusi praktis bagi pelaku UMKM dalam meningkatkan keamanan data penjualan, sekaligus menjadi acuan teknis bagi pengembang sistem untuk mengintegrasikan mekanisme kriptografi pada sistem informasi penjualan.

## 2. Metode Penelitian

### 2.1 Data Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode studi kasus pada Toko Diah Kemasan Kosmetik. Objek penelitian adalah sistem pengelolaan data penjualan yang saat ini disimpan dalam *file Microsoft Excel* tanpa mekanisme pengamanan. Data penelitian berupa laporan penjualan bulanan periode Mei 2023–April 2024, karena hanya data tersebut yang diizinkan untuk digunakan untuk penelitian, dan data mencakup informasi harga sebelum dan sesudah diskon, jumlah pembelian, nama produk, opsi dan waktu pengiriman, waktu pemesanan dan pembayaran, alamat pengiriman, serta total transaksi.

**Tabel 1.** Data Penelitian

Nama File	Jenis File	Ukuran File
Order.completed.20230501_20230531	.xlsx	105KB
Order.completed.20230601_20230630	.xlsx	11KB
Order.completed.20230701_20230731	.xlsx	11KB
Order.completed.20230801_20230831	.xlsx	86KB
Order.completed.20230901_20230930	.xlsx	14KB
Order.completed.20231001_20231031	.xlsx	108KB
Order.completed.20231101_20231130	.xlsx	99KB
Order.completed.20231201_20231231	.xlsx	97KB
Order.completed.20240101_20240131	.xlsx	96KB
Order.completed.20240201_20240229	.xlsx	98KB
Order.completed.20240301_20240330	.xlsx	93KB
Order.completed.20240401_20240430	.xlsx	88KB

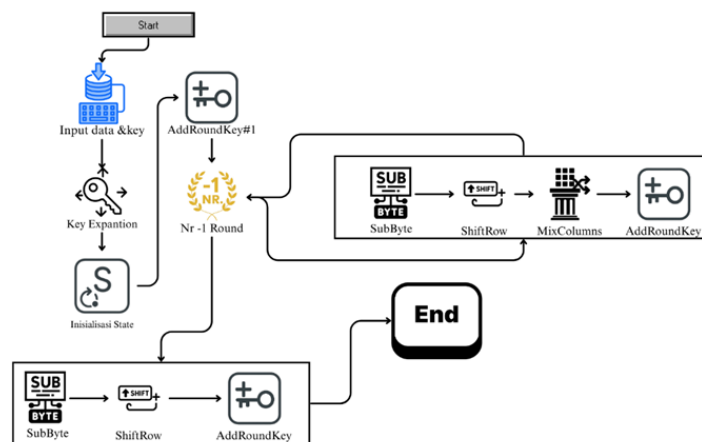
### 2.2 Pengumpulan Data

Data penelitian dikumpulkan melalui observasi langsung di Toko Diah Kemasan Kosmetik untuk mengidentifikasi alur operasional dan kelemahan sistem pengelolaan data, yang menunjukkan bahwa proses pemesanan, komunikasi dengan pemasok, serta pencatatan penjualan masih dilakukan secara manual menggunakan *Microsoft Excel* tanpa perlindungan keamanan. Wawancara hanya dilakukan dengan pemilik toko mengonfirmasi kerentanan tersebut dan menegaskan perlunya sistem keamanan data yang lebih terstruktur.

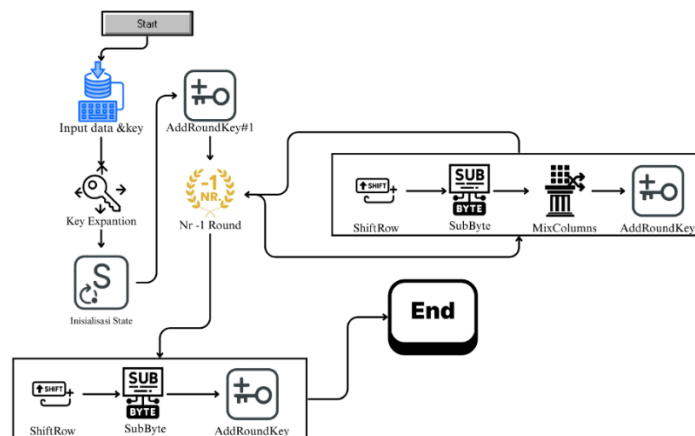
Selain itu, studi pustaka dilakukan untuk mempelajari teori dan temuan penelitian terdahulu terkait kriptografi, khususnya algoritma AES, sebagai dasar pengembangan sistem pengamanan informasi digital yang diusulkan.

### 2.3 Penerapan Algoritma

Penerapan metode penelitian ini bertujuan mengimplementasikan algoritma kriptografi AES-128 dalam sistem pengamanan data penjualan melalui tahapan terstruktur mulai dari pengumpulan data hingga proses enkripsi dan dekripsi. Data diperoleh dari laporan penjualan bulanan yang disediakan pihak toko sebagai bahan uji aplikasi. Implementasi dilakukan dengan memilih file yang akan dienkripsi, mengubah informasi pada *file* (*plaintext*) menjadi bentuk tidak terbaca (*ciphertext*) melalui modifikasi urutan *round* enkripsi menggunakan kunci tertentu, kemudian mengembalikan *ciphertext* ke bentuk semula (*plaintext*) pada tahap dekripsi menggunakan kunci yang sama dengan modifikasi urutan *round* dekripsi. Agar lebih jelas dapat dilihat pada gambar dibawah:

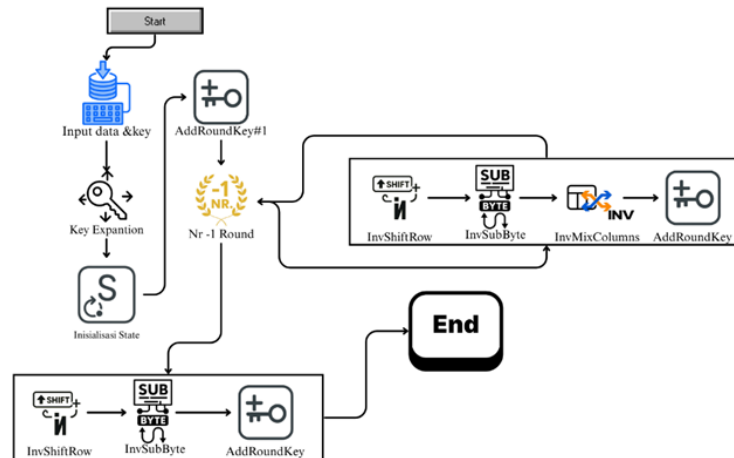


**Gambar 1.** Round enkripsi AES-128 sebelum modifikasi

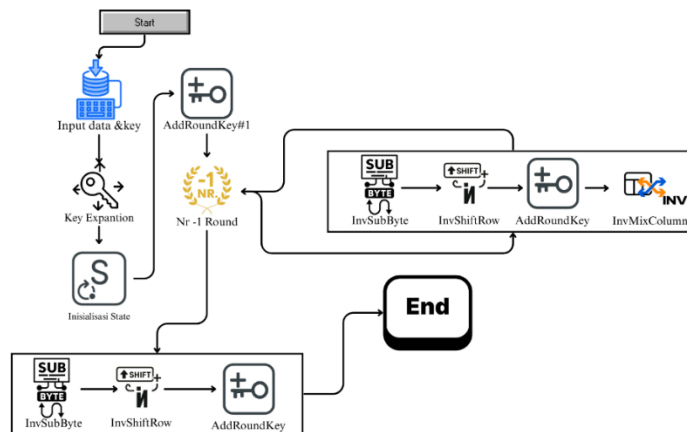


**Gambar 2.** Round enkripsi AES-128 sesudah modifikasi

Gambar diatas menjelaskan proses dari algoritma AES-128 yang telah dimodifikasi dalam melakukan enkripsi. Dimulai dengan *AddRoundKey* yang artinya *initial* round. Setiap *round* akan melakukan *round* yang berulang yaitu *ShiftRow*, *SubByte*, *MixColumns*, dan *AddRoundKey*. Proses ini akan terus diulang sebanyak 10 kali, dilanjutkan dengan final round yang mengulang sekali lagi proses *ShiftRow*, *SubByte*, dan *AddRoundKey*. Susunan operasi dari *SubByte* dan *ShiftRow* ditukar sehingga pihak lain tidak dapat mengakses dengan mudah diweb yang berbeda.



Gambar 3. Round Dekripsi AES-128 sebelum modifikasi



Gambar 4. Round Dekripsi AES-128 sesudah modifikasi

Proses dekripsi pada AES-128 memiliki alur serupa dengan enkripsi, namun menggunakan *inverse function* yang mencakup *InvSubByte* untuk memetakan byte dengan tabel *invers* S-box, *InvShiftRow* untuk menggeser byte ke kanan sebagai kebalikan dari *ShiftRow*, serta *InvMixColumns* untuk mengalikan setiap kolom pada *state* dengan matriks *invers* dalam AES. Susunan operasi dari *InvShiftRow* dan *InvSubByte* ditukar agar dapat dilakukan dekripsi.

## 2.4 Rancangan Pengujian

Rancangan pengujian pada penelitian ini menggunakan metode *black box* untuk menilai kesesuaian fungsi sistem dengan spesifikasi yang ditetapkan, dengan cara memberikan berbagai kombinasi input dan mengamati kesesuaian *output* yang dihasilkan tanpa memeriksa kode sumber. Pengujian dilakukan melalui evaluasi antarmuka pengguna (*user interface*) guna memastikan seluruh fitur berjalan sesuai fungsi dan memenuhi kebutuhan yang telah ditentukan.

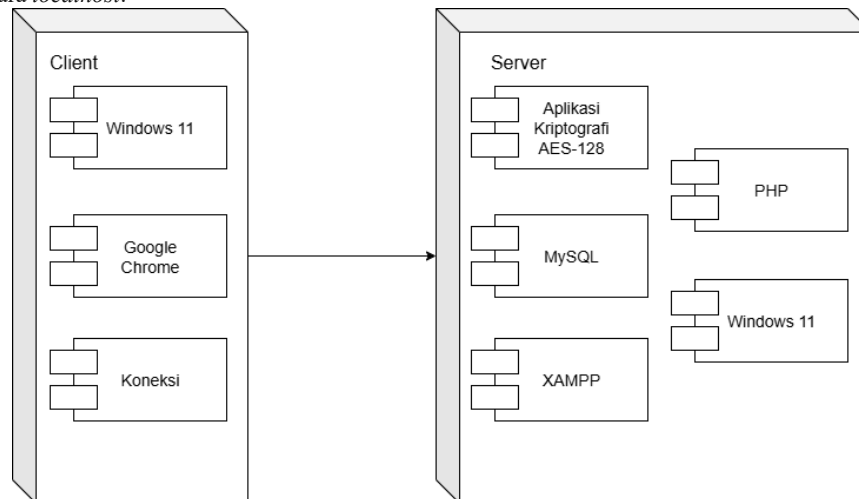
Tabel 2. Rancangan Pengujian *User Interface*

No	Pengujian	Hasil Yang Diharapkan
1	Tombol Login	User dapat masuk setelah mengisi username dan password, user berhasil masuk ke halaman dashboard
2	Tombol Dashboard	User dapat diarahkan ke halaman beranda
3	Tombol enkripsi	User akan ditampilkan halaman enkripsi
4	Memilih berkas yang akan di enkripsi	User akan memilih file dari penyimpanan yang akan di enkripsi
5	Melakukan enkripsi	Setelah memasukan password, User dapat menekan tombol enkripsi
6	Tombol dekripsi	Tampil halaman yang menunjukkan file yang telah di enkripsi
7	Memilih file yang akan di dekripsi	User dapat menekan tombol dekripsi file
8	Melakukan dekripsi file	User dapat memasukan password dan menekan tombol dekripsi file
9	Pencarian berkas	User dapat mencari berkas yang ada pada dashboard
10	Mengunduh berkas	User dapat melakukan download pada dashboard setelah menekan tombol didekripsi atau terenkripsi
11	Tombol logout	User dapat menekan tombol logout untuk menyelesaikan sesi

### 3. Hasil Dan Pembahasan

#### 3.1 Lingkungan Percobaan

Lingkungan percobaan dirancang untuk mereplikasi kondisi operasional Toko Diah Kemasan Kosmetik, sehingga implementasi dan pengujian sistem dapat mencerminkan kinerja nyata dalam pengelolaan dan pengamanan data penjualan. Sistem diuji dengan cara *localhost*.



Gambar 5. Pengaturan Lingkungan Percobaan

#### 3.2 Spesifikasi Sistem

Spesifikasi sistem disesuaikan untuk memenuhi kebutuhan teknis dan memastikan aplikasi berjalan optimal, mencakup konfigurasi perangkat keras dan perangkat lunak yang mendukung fungsionalitas yang telah dirancang.

##### 3.2.1 Spesifikasi Perangkat Keras

Spesifikasi perangkat keras yang digunakan untuk implementasi aplikasi ini adalah sebagai berikut:

- Intel (R) Core (TM) i5-8520U CPU @ 1.60GHz
- RAM 8 GB
- SSD 238 GB

### 3.2.2 Spesifikasi Perangkat Lunak

Spesifikasi perangkat lunak yang ter-install dan penulis menggunakan untuk menjalankan implementasi aplikasi ini adalah sebagai berikut:

- Sistem Operasi *Microsoft Windows 11*
- MySQL
- Xampp*
- Google Chrome*
- Software* pengembangan menggunakan *Visual Studio Code*

### 3.3 Pengujian Aplikasi

Pengujian *black box* menunjukkan bahwa seluruh fitur utama—termasuk login, navigasi *dashboard*, pemilihan *file*, proses enkripsi dan dekripsi, pencarian, serta *logout*—berfungsi sesuai spesifikasi. Proses enkripsi menghasilkan *ciphertext* yang tidak dapat dibaca tanpa kunci, sedangkan dekripsi mengembalikan data ke bentuk *plaintext* asli. Pengujian terhadap 12 *file* penjualan memperlihatkan waktu enkripsi berkisar 1.117–4.267 ms dengan kenaikan ukuran file relatif kecil (0–1,4%). Proses dekripsi berlangsung 940–4.364 ms tanpa perubahan ukuran file, menunjukkan efisiensi dan konsistensi data. Berikut ini adalah hasil dari pengujian aplikasi setelah melakukan serangkaian pengujian pada aplikasi tersebut:

#### 3.3.1 Hasil Pengujian Proses Enkripsi File

Hasil pengujian proses enkripsi file dapat dilihat pada gambar di bawah ini:

**Tabel 3.** Hasil Pengujian Proses Enkripsi File

No	Nama File	Waktu Enkripsi (ms)	Ukuran file sebelum Enkripsi (byte)	Ukuran file setelah Enkripsi	Kenaikan ukuran file (byte)	Kenaikan presentase ukuran file (%)
1	Order.completed.20230501_20230531.xlsx	4.267	107.095	107.104	0,009	0,9%
2	Order.completed.20230601_20230630.xlsx	1.223	10.629	10.640	0,011	1,1%
3	Order.completed.20230701_20230731.xlsx	1.223	11.133	11.136	0,003	0,3%
4	Order.completed.20230801_20230831.xlsx	4.002	87.513	87.520	0,007	0,7%
5	Order.completed.20230901_20230930.xlsx	1.117	13.574	13.584	0,010	1,0%
6	Order.completed.20231001_20231031.xlsx	3.909	109.705	109.712	0,007	0,7%
7	Order.completed.20231101_20231130.xlsx	3.684	101.262	101.264	0,002	0,2%
8	Order.completed.20231201_20231231.xlsx	3.612	98.425	98.432	0,007	0,7%
9	Order.completed.20240101_20240131.xlsx	3.513	97.618	97.632	0,014	1,4%
10	Order.completed.20240201_20240229.xlsx	3.483	100.101	100.112	0,011	1,1%
11	Order.completed.20240301_20240330.xlsx	3.290	95.191	95.200	0,009	0,9%
12	Order.completed.20240401_20240430.xlsx	3.255	89.264	89.264	-	0,0%

#### 3.3.2 Hasil Pengujian Proses Dekripsi File

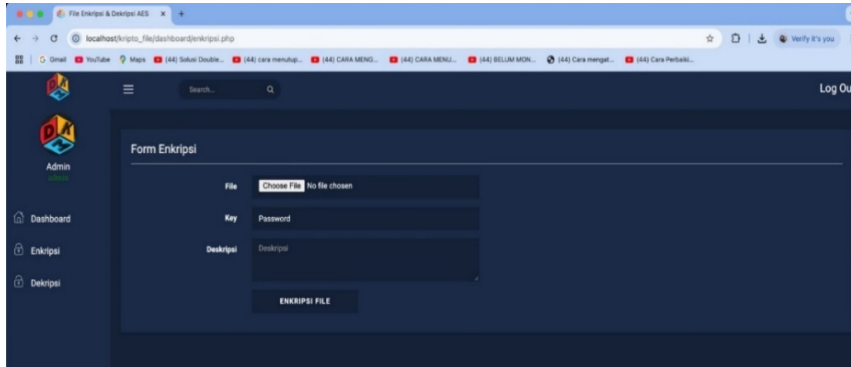
Hasil dari pengujian proses dekripsi file dapat dilihat pada table di bawah ini:

**Tabel 4.** Hasil Pengujian Proses Dekripsi File

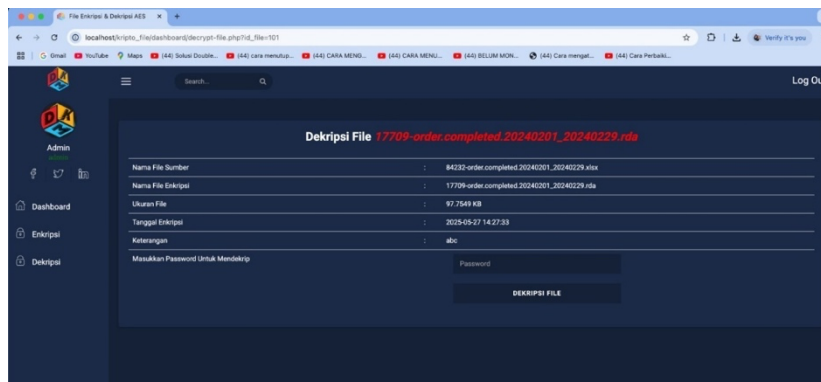
No	Nama File	Waktu Dekripsi (ms)	Ukuran file sebelum dekripsi	Ukuran file setelah dekripsi	Kenaikan/ Penurunan ukuran file
1	58462-order.completed.20230501_20230531.rda	4.364	107.104	107.104	Tidak Berubah
2	81875-order.completed.20230601_20230630.rda	1.024	10.640	10.640	Tidak Berubah
3	78114-order.completed.20230701_20230731.rda	940	11.136	11.136	Tidak Berubah
4	15301-order.completed.20230801_20230831.rda	3.332	87.520	87.520	Tidak Berubah
5	11806-order.completed.20230901_20230930.rda	1.112	13.584	13.584	Tidak Berubah
6	55533-order.completed.20231001_20231031.rda	3.982	109.712	109.712	Tidak Berubah
7	8424-order.completed.20231101_20231130.rda	3.856	101.264	101.264	Tidak Berubah
8	92463-order.completed.20231201_20231231.rda	3.713	98.432	98.432	Tidak Berubah
9	98738-order.completed.20240101_20240131.rda	3.335	97.632	97.632	Tidak Berubah

10	56555-order.completed.20240201_20240229.rda	4.146	100.112	100.112	Tidak Berubah
11	37208-order.completed.20240301_20240330.rda	3.681	95.200	95.200	Tidak Berubah
12	49239-order.completed.20240401_20240430.rda	3.405	89.264	89.264	Tidak Berubah

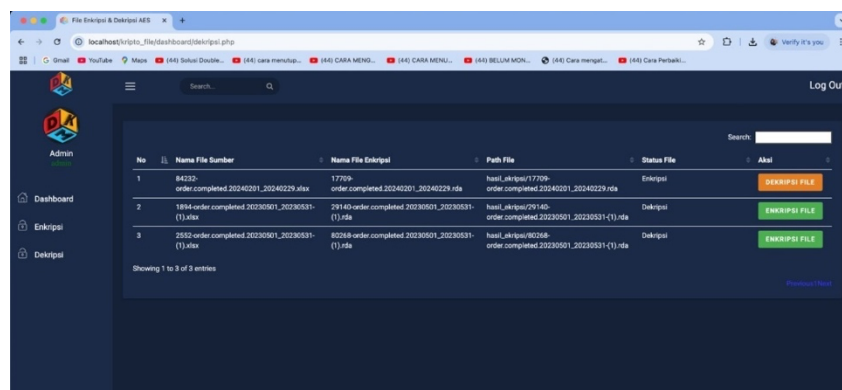
Ekstensi *file* .rda menunjukkan bahwa *file* telah dienkripsi.



**Gambar 6.** Form Proses Enkripsi



**Gambar 7.** Form Proses Dekripsi File



**Gambar 8.** Form Dekripsi

### 3.4 Analisis Hasil

Keberhasilan enkripsi-dekripsi membuktikan bahwa penerapan AES-128 efektif menjaga kerahasiaan data penjualan, selaras dengan temuan studi sebelumnya bahwa AES-128 memiliki tingkat keamanan tinggi dan kinerja baik untuk data bisnis berskala kecil hingga menengah. Kenaikan ukuran file yang minimal menegaskan efisiensi algoritma terhadap sumber daya penyimpanan. Namun, percobaan dekripsi menggunakan platform eksternal gagal memulihkan data karena operasi telah ditukar, yang mengindikasikan pentingnya kesesuaian

konfigurasi parameter (mode operasi, padding, format kunci) dalam interoperabilitas lintas sistem. Jika dibandingkan dengan AES-256, AES-128 memberikan keseimbangan yang lebih baik antara keamanan dan kecepatan pemrosesan pada skala data yang sama, sebagaimana dibahas dalam [Ridho & Romli, 2024]

### 3.5 Kelebihan dan Keterbatasan

Aplikasi ini memiliki keunggulan berupa antarmuka sederhana, proses enkripsi cepat, dan keamanan berbasis algoritma yang diakui secara internasional. Namun, keterbatasan terletak pada absennya sistem pemulihan kunci dan pembatasan format file yang didukung, serta penurunan kinerja pada file berukuran besar di atas 3mb dibutuhkan waktu lebih dari 1 menit. Secara akademik, penelitian ini memberikan kontribusi pada implementasi praktis AES-128 di lingkungan usaha mikro, kecil, dan menengah (UMKM), serta menjadi referensi untuk pengembangan sistem keamanan data dengan kompatibilitas dan fitur pemulihan yang lebih baik, termasuk pengembangan dukungan untuk algoritma AES-256 yang menawarkan tingkat keamanan lebih tinggi bagi kebutuhan data berskala besar atau sensitif.

## 4. KESIMPULAN

Penelitian ini menunjukkan bahwa implementasi algoritma kriptografi AES-128 pada sistem pengamanan data penjualan di Toko Diah Kemasan Kosmetik berhasil dilakukan dengan baik. Pengujian *black box* membuktikan bahwa seluruh fungsi utama aplikasi berjalan sesuai spesifikasi, dan algoritma mampu menjaga kerahasiaan serta integritas data transaksi yang sebelumnya disimpan dalam format terbuka dan rentan penyalahgunaan. Temuan ini menjawab tujuan penelitian untuk merancang dan menguji sistem keamanan data berbasis AES-128 yang efektif bagi lingkungan UMKM, sekaligus memperkuat bukti empiris tentang keandalan AES-128 dalam aplikasi bisnis berskala kecil hingga menengah.

Secara praktis, sistem ini memberikan solusi keamanan yang dapat diadopsi UMKM untuk melindungi informasi penjualan dari akses tidak sah. Namun, penelitian ini memiliki keterbatasan pada absennya manajemen kunci yang aman, fitur *backup* dan *recovery*, serta mekanisme autentikasi ganda. Arah penelitian selanjutnya dapat difokuskan pada pengembangan fitur keamanan tambahan, peningkatan interoperabilitas dengan sistem eksternal, serta pengujian pada volume data yang lebih besar untuk menguji skalabilitas dan ketahanan sistem.

## DAFTAR PUSTAKA

- [1] S. William, *Kriptografi dan Keamanan Jaringan : Prinsip dan Praktik (edisi ke-7, 7th ed.* Pearson, 2017).
- [2] J. Daemen and V. Rijmen, *Desain Rijndael: AES - Standar Enkripsi Lanjutan.* Springer, 2002.
- [3] B. A. Forouzan, *Kriptografi dan Keamanan Jaringan*, 1 jilid 1. McGraw - Hill Education, 2008.
- [4] M. A. Hidayah, N. B. S. K. M. kom Nugroho, and M. S. K. M. K. Iswan, "Penerapan Kriptografi Menggunakan Algoritma AES Untuk Keamanan Data Penjualan Pada PT. Mestika Sakti," *Jurnal CyberTech*, 2020, doi: <https://doi.org/10.53513/jct.v1i3.1901>.
- [5] M. W. Ramadhana, A. Muhazir, and J. Prayudha, "Pengamanan Data Penjualan Biji Kopi Sembekandua Menggunakan Metode Advanced Encryption Standard," *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD)*, vol. 3, no. 2, pp. 252–262, Mar. 2024, doi: 10.53513/jursi.v3i2.6092.
- [6] A. Tumanggor, H. Rumapea, and A. P. Silalahi, "Implementasi Algoritma AES Pada Keamanan Dokumen Keuangan (CV. Multikreasi Bersama)," *Jurnal Ilmiah Teknik Informatika* Apr. 2023, Medan.
- [7] T. A. Ramadhani, A. F. Cobantoro, and S. Sugianti, "Implementasi Algoritma Advanced Encryption Standard 128 untuk Pengamanan Database Sistem Registrasi Pasien," *Jurnal Informatika Polinema*, vol. 10, no. 4, pp. 521–526, Aug. 2024, doi: 10.33795/jip.v10i4.5619.
- [8] M. R. Andriyanto and P. Sukmasetya, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace," *Journal of Computer System and Informatics (JoSYC)*, vol. 4, no. 1, pp. 179–187, Dec. 2022, doi: 10.47065/josyc.v4i1.2451.
- [9] M. R. Rizky and T. Fatimah, "Implementasi Kriptografi Algoritme AES-128 Untuk Pengamanan Data penjualan Dan Pembelian Mobil Pada Showroom BOB'S Auto," *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, pp. 242–250, 2023, doi: <https://senafiti.budiluhur.ac.id/index.php/senafiti/index>.
- [10] D. Widyawan and I. Imelda, *Pengamanan File Menggunakan Kriptografi Dengan Metode AES-128 Berbasis WEB di Komite Nasional Keselamatan Transportasi*, vol. 4 No 1, Sistem Komputer dan Teknik Informatika (SKANIKA), 2021.