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

IMPLEMENTASI KRIPTOGRAFI ALGORITME AES-128 UNTUK PENGAMANAN DATA PENJUALAN DAN PEMBELIAN MOBIL PADA SHOWROOM BOB'S AUTO

Muhammad Reza Rizky[1*], Titin Fatimah[2]

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

Email: [1*]1911501409@student.budiluhur.ac.id, [2]titin.fatimah@budiluhur.ac.id
(* : corresponding author)

Abstrak- Showroom Bob's Auto memiliki masalah untuk menyimpan data penting yang rapih dan aman. Showroom Bob's Auto adalah usaha jual dan beli mobil bekas yang sudah cukup lama berdiri. Untuk menyimpan data penjualan, pembelian dan lainnya harus memiliki suatu aplikasi pengamanan data. Supaya tidak terjadi kehilangan atau kebocoran data pada showroom dibutuhkan suatu aplikasi atau web untuk mengamankan datanya. Kriptografi adalah teknik pengamanan informasi yang melibatkan pengolahan informasi awal (plaintext) menggunakan sebuah kunci dalam proses enkripsi. Hal tersebut dapat menghasilkan pesan baru yang disebut ciphertext, yang untuk membacanya tidak dapat secara langsung. Untuk mengembalikan ciphertext menjadi informasi awal, diperlukan proses deskripsi yang menggunakan kunci yang sama. Dengan demikian, kriptografi memungkinkan pengamanan informasi melalui proses enkripsi dan deskripsi. Dengan kriptografi bisa menjaga kerahasiaan file penting dari Showroom Bob's Auto. Kriptografi yang digunakan akan memakai metode "Advanced Encryption Standard" (AES-128). Metode "Advanced Encryption Standard (AES-128) adalah sebuah algoritme kriptografi simetris yang secara luas digunakan untuk melindungi keamanan data dalam berbagai aplikasi dan protokol. Algoritme ini menggabungkan beberapa transformasi matematis seperti penggantian byte, pertukaran baris, dan pemetaan ke matriks Galois untuk enkripsi dan dekripsi data.

Kata Kunci: showroom bob's auto, kriptografi, advanced encryption standard (AES-128), plaintext, ciphertext, enkripsi dan dekripsi.

IMPLEMENTATION OF AES-128 CRYPTOGRAPHY ALGORITHM TO SECURE CAR SALES AND PURCHASE DATA AT BOB'S AUTO SHOWROOM

Abstract- *Bob's Auto Showroom has trouble keeping important data neat and secure. Bob's Auto Showroom is a used car buying and selling business that has been around for a long time. To store data on sales, purchases and others, you must have a data security application. In order not to lose or leak data in the showroom, an application or web is needed to secure the data. Cryptography is an information security technique that involves processing initial information (plaintext) using a key in the encryption process. It can generate a new message called ciphertext, which cannot be read directly. To return the ciphertext to the initial information, a description process is required that uses the same key. Thus, cryptography allows information security through the process of encryption and description. With cryptography you can maintain the confidentiality of important files from the Bob's Auto Showroom. The cryptography used will use the "Advanced Encryption Standard" (AES-128) method. The "Advanced Encryption Standard (AES-128) method is a symmetric cryptographic algorithm that is widely used to protect data security in various applications and protocols. This algorithm incorporates several mathematical transformations such as byte substitution, row swapping, and mapping to the Galois matrix for data encryption and decryption.*

Keywords*: showroom bob's auto, cryptography, advanced encryption standard (AES-128), plaintext, ciphertext, encryption and decryption.*

1. PENDAHULUAN

Showroom Bob's Auto adalah sebuah perusahaan yang bergerak di bidang penjualan mobil bekas. Namun, perusahaan ini menyadari bahwa sistem pencatatan data secara manual memiliki keterbatasan yang dapat mempengaruhi akurasi data dan pengamanan data. Oleh karena itu, Showroom Bob's Auto ingin beralih ke sistem pencatatan yang lebih canggih untuk meningkatkan pengelolaan data, serta mengantisipasi kemungkinan kehilangan data yang masih dilakukan secara manual, yaitu menyimpan file penjualan dan pembelian mobil ke

dalam arsip tempat penyimpanan berkas maupun dalam penyimpanan di harddisk pada komputer. Hal ini pernah terjadi ketika pembeli memprotes adanya kerusakan pada mobil namun file yang sudah dibuat saat penjualan yang berisi data mobil dan pemilik sebelumnya hilang.

Dengan mempertimbangkan keterbatasan sistem manual, perkembangan teknologi, serta kebutuhan untuk mengantisipasi kehilangan data, muncul suatu ide yang tertuju dari permasalahan yang ada, yaitu untuk merancang sistem keamanan yang dapat digunakan untuk melindungi data berupa file dengan teknik kriptografi serta pembuatan pencatatan data pada berbasis web. perusahaan ini berharap untuk meningkatkan akurasi serta kualitas pengelolaan data penjualan dan pembelian mobil, serta menjaga keamanan data tersebut.

Oleh karena itu, untuk meningkatkan efisiensi operasional dan menjaga keamanan data penjualan dan pembelian mobil Showroom Bob's Auto menggunakan teknik kriptografi untuk mengenkripsi data dan mencegah akses yang tidak berwenang.

Kriptografi adalah bidang ilmu dan teknologi yang berhubungan dengan keamanan informasi melalui proses penyandian (enkripsi) dan penyandian kembali (dekripsi). Tujuan utama dari enkripsi adalah melindungi kerahasiaan, integritas, dan keaslian data selama proses penyimpanan, transmisi, dan pengolahan. Informasi atau pesan yang ingin dijamin keamanannya melalui enkripsi disebut sebagai plaintext atau teks biasa. Proses mengubahnya menjadi bentuk yang tidak terbaca disebut enkripsi, dan hasilnya dikenal sebagai ciphertext atau teks terenkripsi. Enkripsi melibatkan penggunaan algoritme enkripsi yang mengubah plaintext menjadi ciphertext dengan menggunakan kunci enkripsi yang tepat. Untuk membaca kembali pesan yang telah terenkripsi, dilakukan proses dekripsi dengan menggunakan kunci dekripsi yang sesuai untuk mengembalikan ciphertext menjadi plaintext.[1]

AES-128 (Advanced Encryption Standard 128-bit) adalah algoritme enkripsi simetris yang digunakan untuk mengenkripsi dan mendekripsi data. AES-128 menggunakan kunci 128-bit, artinya kunci yang dapat digunakan untuk enkripsi dan dekripsi panjangnya mencapai 128 bit.[2]

Penelitian terdahulu telah membahas enkripsi kriptografi dengan metode AES-128 berbasis web dari "Dian widyawan & Imelda" pada tahun 2021 dengan judul "Pengamanan file menggunakan kriptografi dengan metode AES-128 berbasis web di Komite Nasional Keselamatan Transportasi". Pada penelitian ini kontribusinya mengamankan data penjualan dan data pembelian berbasis web dengan metode AES-128 CBC pada Showroom Bob's Auto. Perbedaan dari jurnal diatas, yaitu ada pada metode yang digunakan. Penelitian ini menggunakan metode AES-128 yang dimodifikasi dengan operasi CBC.

AES-128 CBC (Cipher Block Chaining) adalah sebuah mode operasi kriptografi yang digunakan bersama dengan algoritme AES-128 untuk mengamankan data dalam bentuk ciphertext (teks terenkripsi). Keuntungan dari AES-128 CBC adalah memberikan tingkat keamanan lebih pada data yang memiliki pola yang sama dan menyediakan proteksi terhadap serangan kriptoanalisis tertentu. Namun, perlu diingat bahwa vektor inisialisasi (IV) harus dipilih secara acak dan unik untuk setiap pesan yang dienkripsi untuk menjaga keamanan sistem. [3]

2. METODE PENELITIAN

A. Studi Literatur

Pada tahapan studi literatur, dilakukan *review* terhadap berbagai penelitian sebelumnya, diantaranya adalah Kriptografi file metode *transposition cipher* pengaman pesan, AES berbasis *web* di KNKT, AES untuk Penyandian SMS, AES berbasis *web* pada *e-mail*, AES-128 dan RC4 pada *web* tes masuk karyawan, AES & Rabin pada database, AES & *caesar cipher* untuk *File* teks, AES pada peningkat keamanan dari serangan *brute force*, AES & LSB pada citra *digital*, AES pada penyandian *file* dokumen.

B. Penerapan Metode

Untuk memastikan pencapaian tujuan yang telah ditetapkan sebelumnya, metode AES-128 digunakan sebagai pedoman utama dalam pelaksanaan penelitian ini. Metode ini memiliki kunci enkripsi dengan panjang 128 bit yang memungkinkan perlindungan data dengan tingkat keamanan yang tinggi.

Implementasi AES-128 melibatkan beberapa langkah utama. Pertama, data terenkripsi dibagi menjadi blok 128-bit. Setiap blok data kemudian diubah menggunakan serangkaian operasi matematika yang kompleks.

Proses enkripsi AES-128 melibatkan penggunaan kunci enkripsi yang sama untuk setiap blok data. Kunci enkripsi ini dihasilkan dari kunci utama yang harus dirahasiakan. Dalam enkripsi, blok data dan kunci enkripsi digabungkan dalam operasi yang disebut "XOR" (eXclusive OR).[4]

Selanjutnya, langkah-langkah seperti substitusi, pergeseran, dan pencampuran dilakukan pada blok data dengan menggunakan tabel khusus dan operasi matematika. Proses ini berulang secara berurutan pada setiap blok data untuk menghasilkan data terenkripsi.[5]

Proses dekripsi AES-128 hampir sama dengan proses enkripsi, namun urutan operasinya dibalik. Data terenkripsi dibagi menjadi blok-blok dan setiap blok diubah menggunakan operasi matematika yang merupakan kebalikan dari proses enkripsi. Kunci enkripsi yang sama digunakan untuk mengembalikan data ke bentuk aslinya.[6]

C. Analisis sistem

1. Analisis Data

   Salah satu langkah untuk mengatasi masalah keamanan ini, dalam analisis data, adalah mengumpulkan file-file yang digunakan untuk mendapatkan informasi yang dibutuhkan untuk merancang program. Kumpulan file menurut jenisnya. Dekripsi File menentukan langkah-langkah yang digunakan untuk membuat aplikasi yang mudah dipahami.

2. Analisis sistem.

   Pengamanan yang digunakan pada sistem adalah proses enkripsi isi file. Enkripsi dilakukan untuk mengamankan isi file rahasia (hanya pihak yang berwenang yang dapat mengaksesnya). Karena membutuhkan modul untuk mengenkripsi data. Modul enkripsi yang ditempatkan di aplikasi akan dipanggil saat pengguna mengamankan konten file. Selama ini, modul dekripsi dipanggil ketika pengguna ingin melihat isi file.

3. Desain Perangkat Lunak

   Pada tahap perancangan sesuai hasil analisis sistem khususnya pada perancangan enkripsi dan dekripsi. Selain itu, dukungan tambahan dibangun ke dalam aplikasi dan desain antarmuka pengguna. Pengembangan sistem ini menggunakan metode waterfall, model ini harus diselesaikan satu per satu secara keseluruhan sebelum melanjutkan ke langkah berikutnya, dan hasil setiap langkah harus dicatat secara akurat.

4. Implementasi

   Dalam implementasi ini, apa yang dikandung pada tahap desain direalisasikan dalam bahasa pemrograman tertentu. Dalam hal ini aplikasi ini digunakan:

   1. Perangkat lunak yang digunakan dalam implementasi pengamanan file data menggunakan bahasa pemrograman PHP dan mysql sebagai databasenya.
   2. Hardware yang digunakan adalah prosesor Intel Core i5 4210U, RAM 8 GB DDR3, HDD 500 GB, VGA Nvidia Geforce 920M.

5. Pemeriksaan Sistem

   Metode pengujian berupa black box yang digunakan untuk mengecek error dan ketika dijalankan, aplikasi akan memperjelas apakah input yang diterima benar dan hasil yang diperoleh benar atau tidak.

6. Kesimpulan

   Tahap akhir ini menyimpulkan bahwa penerapan metode kriptografi Advanced Encryption Standard (AES) 128, berjalan dengan baik, dan dapat mengamankan file data yang dibeli dan dijual di Showroom Bob's Auto aman dan pada tahap ini, ada usulan pengembangan dalam sistem ini.

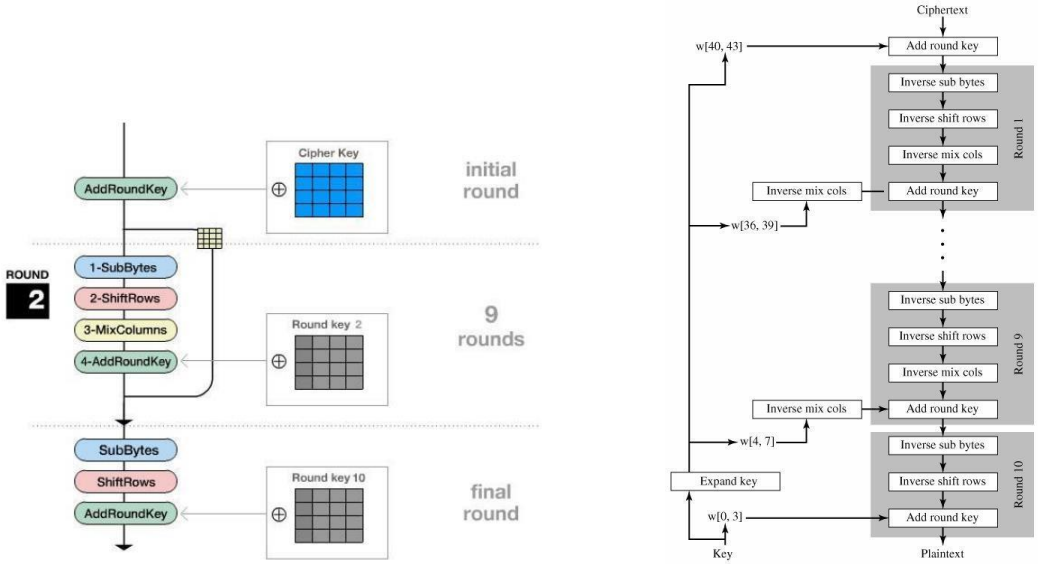
2.1 *Advanced Encryption Standard*

AES menggantikan algoritma kunci data standar DES, AES menggunakan cipher blok simetris. Algoritma AES memiliki panjang kunci yang berbeda dan ukuran blok tetap 128 bit. Untuk enkripsi dan dekripsi, kunci AES128 menggunakan proses pengulangan yang disebut "putaran", yang terdiri dari sepuluh lintasan pola matriks empat kali empat yang masing-masing terdiri dari satu *byte* atau delapan bit. [7].

2.2 Proses Enkripsi

Algoritma AES memiliki empat jenis enkripsi: transformasi *byte*: *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Pada tahap pertama proses enkripsi, input disalin ke dalam ruang status untuk dikonversi menggunakan *byte AddRoundKey*. Kemudian, *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* dikonversi

berulang kali sejumlah Nr. Algoritma ini dikenal sebagai algoritma AES (fungsi putar). Dibandingkan dengan putaran sebelumnya, keadaan state tidak berubah dalam Kolom Campuran; pada putaran terakhir, ada sedikit perubahan [8]. Gambar 1 berikut menunjukkan proses enkripsi AES-128:



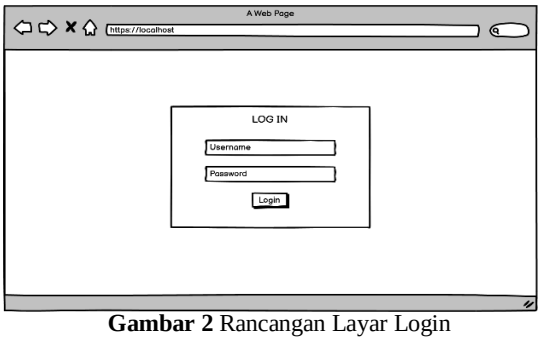
Gambar 1 Proses Enkripsi dan Dekripsi

2.3 Proses Dekripsi

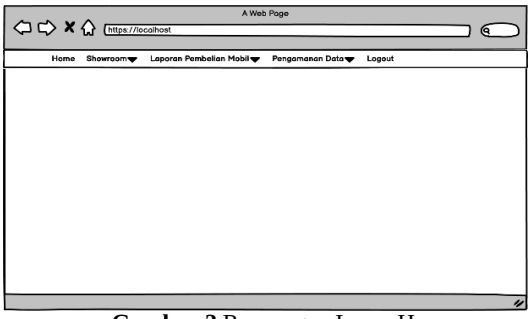
Proses deskripsi dengan metode AES melibatkan transformasi *cipher* yang dapat dibalikkan. Transformasi ini dilakukan dengan urutan terbalik untuk menghasilkan *inverse cipher* yang memudahkan pemahaman algoritma AES [9]. Dalam *invers cipher* terdapat beberapa transformasi *byte* yang digunakan, yaitu *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *InvAddRoundKey*. Transformasi ini berguna untuk mengembalikan data bentuk aslinya setelah proses enkripsi [10]. Proses dekripsi AES-128 dapat dilihat pada gambar 1. berikut:

2.3 Rancangan Layar

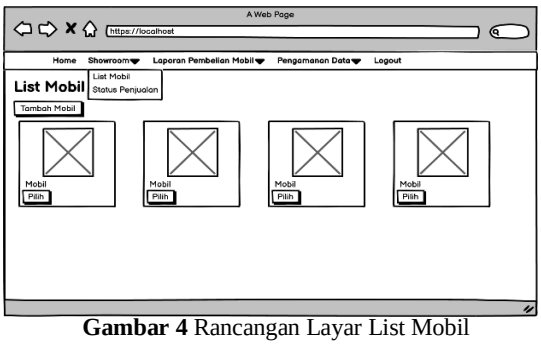
Dalam pembuatan suatu aplikasi, sangat diperlukan tahap perancangan layar sebagai bentuk dasar dalam membuat desain aplikasi yang diinginkan. Rancangan layar harus mudah dimengerti, tujuannya agar pengguna dapat merasa nyaman dan tidak bingung dalam menggunakan aplikasi ini. Perhatikan Gambar 2 berikut:



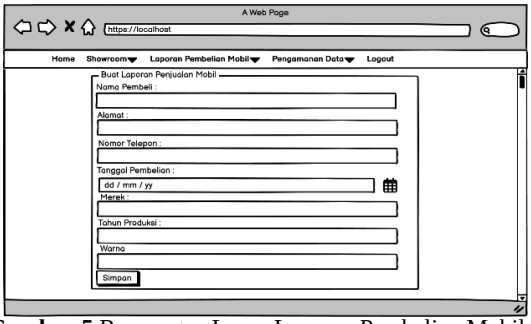
Gambar 2 Rancangan Layar Login



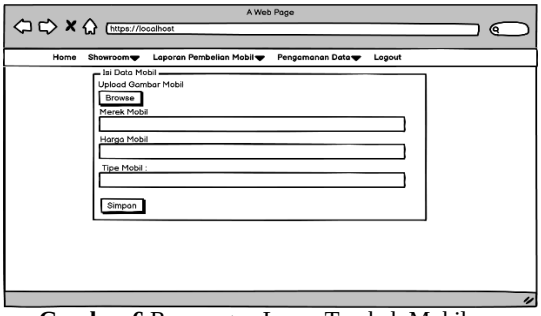
Gambar 3 Rancangan Layar Home



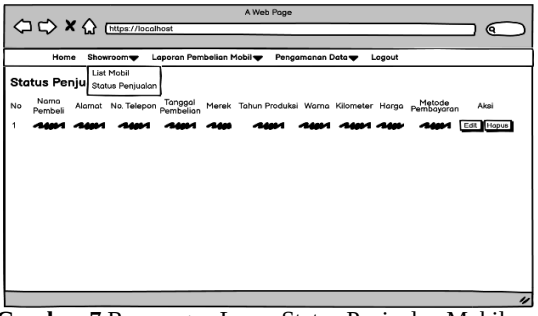
Gambar 4 Rancangan Layar List Mobil



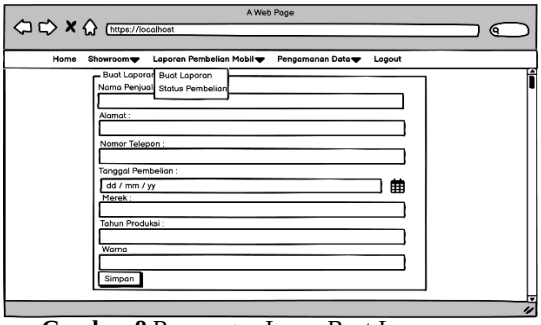
Gambar 5 Rancangan Layar Laporan Pembelian Mobil



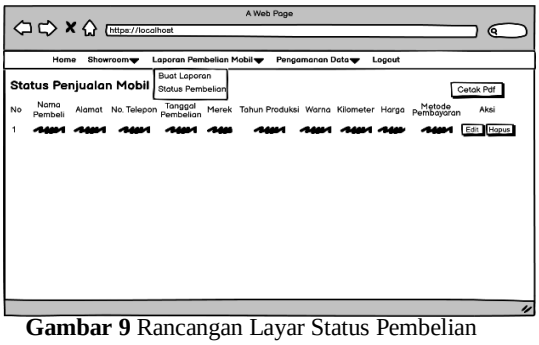
Gambar 6 Rancangan Layar Tambah Mobil



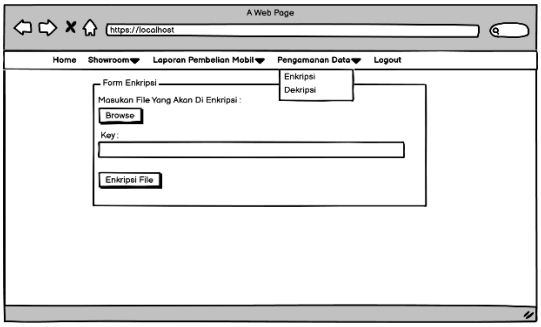
Gambar 7 Rancangan Layar Status Penjualan Mobil



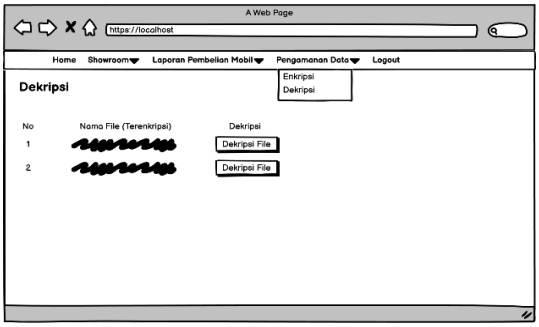
Gambar 8 Rancangan Layar Buat Laporan



Gambar 9 Rancangan Layar Status Pembelian



Gambar 10 Rancangan Layar Enkripsi



Gambar 11 Rancangan Layar Dekripsi

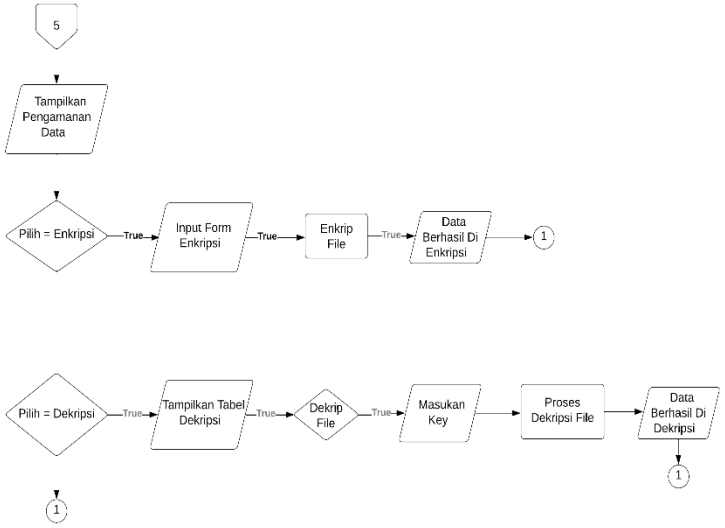
Gambar 2 Rancangan Layar

3. HASIL DAN PEMBAHASAN

Pada bagian ini adalah penjelasan dari implementasi algoritme AES-128 untuk enkripsi dan dekripsi data *showroom*. Bagian ini menjelaskan tentang *flowchart*, algoritme, proses, hasil enkripsi dan dekripsi dokumen dalam sebuah aplikasi.

3.1 Flowchart Menu Enkripsi

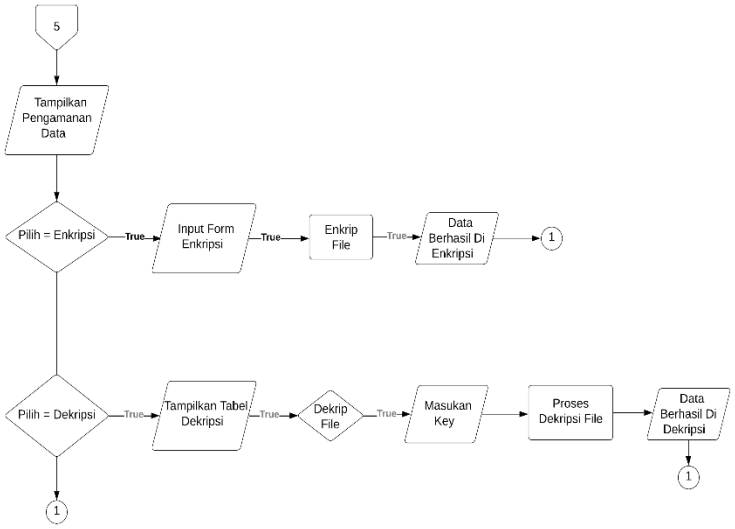
Pada gambar 3. merupakan *flowchart* dari halaman *form* enkripsi, dimana *flowchart* ini menjelaskan tentang melakukan enkripsi file, dalam mengenkripsi file admin harus memasukkan *password*, setelah itu program akan memproses enkripsi.



Gambar 12 *Flowchart* Menu Enkripsi

3.2 *Flowchart* Menu Dekripsi

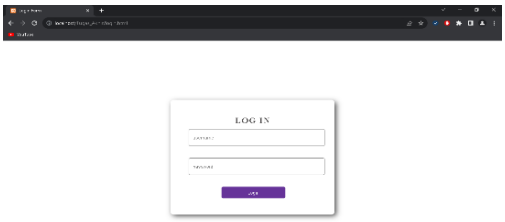
Pada gambar 4 merupakan *flowchart* dari halaman dekripsi, dimana *flowchart* ini menjelaskan tentang melakukan dekripsi file. Dalam dekripsi file admin harus memasukkan *password* yang sesuai dengan enkripsi, setelah itu program akan memproses dekripsi.



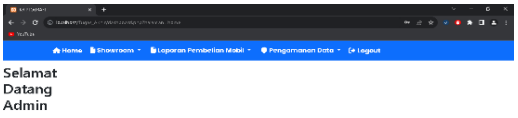
Gambar 13 *Flowchart* Menu Dekripsi

3.3 Tampilan Layar

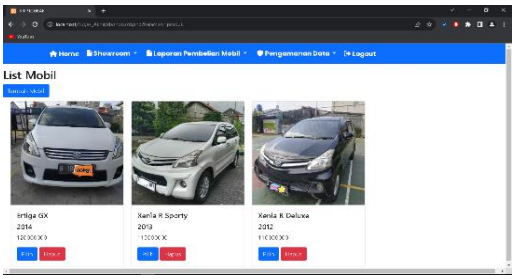
Pada gambar 5 terdapat tampilan layar aplikasi pengamanan data showroom. Pada gambar 5 terdapat tampilan aplikasi login hingga menu dekripsi file.



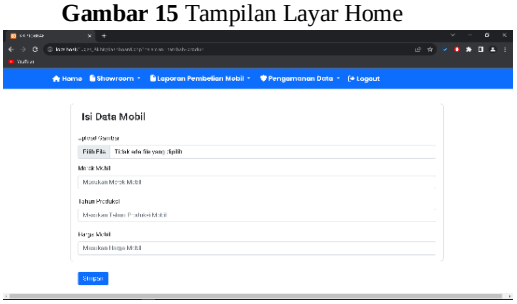
Gambar 14 Tampilan Layar Login



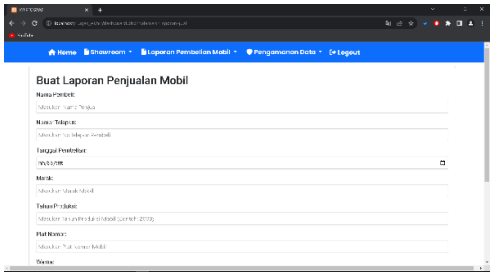
Gambar 15 Tampilan Layar Home



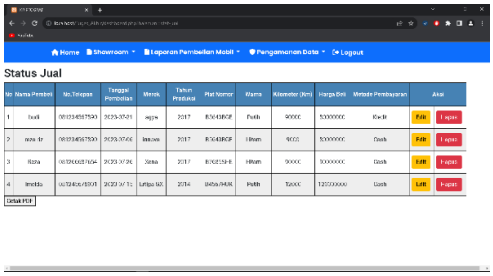
Gambar 16 Tampilan Layar List Mobil



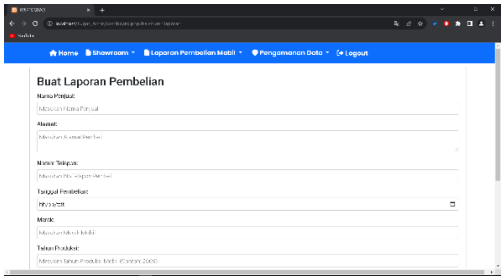
Gambar 17 Tampilan Layar Tambah Mobil



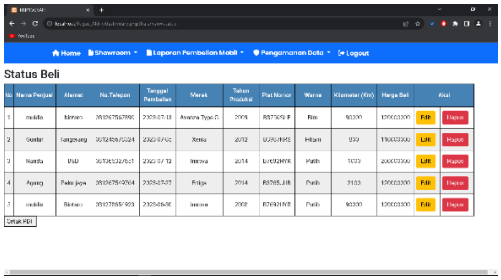
Gambar 18 Tampilan Layar Buat Laporan Penjualan



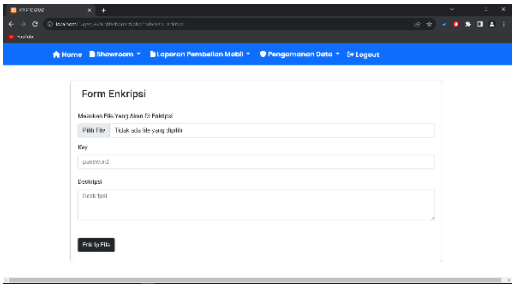
Gambar 19 Tampilan Layar Status Penjualan



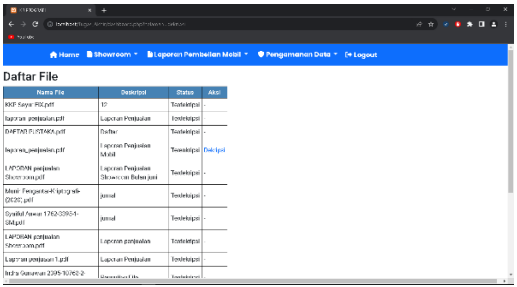
Gambar 20 Tampilan Layar Buat Laporan Pembelian



Gambar 21 Tampilan Layar Status Pembelian



Gambar 22 Tampilan Layar Enkripsi



Gambar 22 Tampilan Layar Dekripsi

3.4 Pengujian

Dari pengujian yang telah dilakukan terdapat sisi kecepatan dan hasil enkripsi yang berupa file tidak bisa dibuka dan beberapa ukuran data sebelum dan sesudah dienkripsi menggunakan algoritme kriptografi AES-128. Tabel 1 menunjukan hasil pengujian yang dilakukan

Tabel 1 Hasil Pengujian Enkripsi dan Dekripsi File

Nama *File*	Ukuran *File* (Kilobyte)			Waktu (Detik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
LAPORAN penjualan Showroom.pdf	63kb	84kb	63kb	1,46 detik	1,23 detik
Laporan_beli.pdf	8kb	10kb	8kb	1,31 detik	1,26 detik
Laporan Pembelian Showroom.pdf	101kb	135kb	101kb	1,35 detik	1,24 detik
Munir Pengantar-Kriptografi-(2020).pdf	3.408kb	4.554kb	3.408kb	2,17 detik	1,75 detik
Syaiful Anwar 1762-3395-1-SM.pdf	721kb	961kb	721kb	1,36 detik	1,25 detik
Indra Gunawan 2395-10768-2-PB.pdf	1.071kb	1.428kb	1.071kb	1,48 detik	1,31 detik
Arif prayitno & Nurdin 55-188-1-PB.pdf	407kb	542kb	407kb	1,32 detik	1,24 detik
Ahmad Rosyadi 19-3530-1-PB.pdf	191kb	255kb	191kb	1,25 detik	1,06 detik
Ahmad Arif &Putri Mandarani Hal 84-93	929kb	1.239kb	929kb	1,45 detik	1,23 detik
Geri Grehasa & Sri Mulyati 464-1213-1-PB-1	556kb	741kb	556kb	1,36 detik	1,24 detik

4. KESIMPULAN

Kriptografi dengan metode AES-128 dapat mengamankan file penting pada Showroom dengan cepat dan aman. Aplikasi ini dapat digunakan untuk menginput data penjualan dan pembelian serta untuk mengamankan file data penjualan dan pembelian pada Showroom Bob's Auto. Dengan memodifikasi proses enkripsi khususnya pada *random key*, aplikasi ini memiliki tingkat keamanan yang tinggi. Aplikasi ini bisa mengamankan *file* pdf.

Metode ini bisa dikembangkan lagi untuk program enkripsi dan dekripsi file ini dengan memodifikasi ataupun mengkombinasikan metode AES-128 dengan metode yang lain supaya sistem semakin sulit untuk diretas. Diharapkan untuk dikembangkan lagi aplikasi ini supaya fleksibilitas dengan membuat versi *mobile* dari aplikasi ini.

DAFTAR PUSTAKA

[1] Imelda & D. Widyawan, "*Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di KNKT*" SKANIKA, vol. 4, no. 1, pp. 15–22, 2021.

[2] A. Prayitno & N. Nurdin, "*Analisa dan implementasi kriptografi pada pesan rahasia menggunakan algoritme cipher transposition*" Jurnal elektronik sistem informasi dan komputer, pp. 1–10, 2017.

[3] A. Arif & P. Mandarani, "*Rekayasa perangka lunak kriptografi menggunakan algoritme advanced encryption standard (AES) 128 bit pada sistem keamanan short message service (SMS) berbasis android*" TEKNOIF , vol. 4, no. 1, pp. 84–93, 2016.

[4] A. Rosyadi, "*Implementasi algoritme kriptografi AES untuk enkripsi dan dekripsi email*" TRANSIENT, vol. 1, no. 3, pp. 63–67, 2012.

[5] G. Grehasen and S. Mulyati, "*Pengamanan Database Pada Aplikasi Test Masuk Karyawan Baru Berbasis Web Menggunakan Algoritme Kriptografi AES-128 Dan RC4*" BIT , vol. 14, no. 1, 2017.

[6] I. Gunawan, "*Peningkatan pengamanan data file menggunakan algoritme kriptografi AES dari serangan brute force*" TECHSI, vol. 13, no. 1, pp. 14–25, 2021.

[7] S. Anwar, "*Implementasi pengamanan data dan informasi dengan metode steganografi LSB dan algoritme kriptografi AES*" Seminar Nasional Teknologi Informasi dan Multimedia , pp. 3–8, 2017.

[8] A. Fitrah Marisman and A. Hidayati, "*Pembangunan aplikasi pembanding kriptografi dengan Caesar cipher dan advanced encryption standard (AES) untuk file teks*" Jurnal Penelitian Komunikasi dan Opini Publik , vol. 19, no. 3, pp. 213–222, 2015..

[9] R. Munir, "*Pengantar Kriptografi*" Kriptografi Informatika ITB, 2019.

[10] 2021, G. Istia, SCRIBD. Available: https//www.scribd.com/document/507369841/IMK#.