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 MENGGUNAKAN AES-128 UNTUK MENGAMANKAN DATA PENJUALAN DAN PEMBELIAN PADA SHOWROOM BAROQAH MOBIL

Boby Saskia Dwi Saputra[1*], Mohammad Syafrullah[2]

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

Email: [1*]bobysds20@gmail.com, [2]mohammad.syafrullah@budiluhur.ac.id
(: corresponding author)*

Abstrak- Showroom Mobil Baroqah adalah perusahaan dagang otomotif yang sudah lama berdiri. Untuk menyimpan penjualan, pembelian, dan data lainnya, Anda memerlukan aplikasi keamanan data. Penelitian ini menggunakan metode pengumpulan data, yaitu dengan melakukan observasi dan survey langsung ke lokasi penelitian (observasi), dengan melakukan sesi tanya jawab langsung pada narasumber (wawancara) dan dengan cara mencatat dengan membaca buku pedoman. Hasil penelitian menunjukkan bahwa program terkait keamanan data penjualan diperlukan untuk showroom. Agar data di showroom tidak hilang atau bocor, maka perlu adanya aplikasi atau website untuk mengamankan data. Kriptografi adalah teknik keamanan informasi yang melibatkan pemrosesan informasi asli (teks yang jelas) menggunakan kunci dalam proses enkripsi. Ini dapat menghasilkan pesan baru yang disebut ciphertext, yang tidak dapat dibaca secara langsung. Untuk mengembalikan ciphertext ke informasi aslinya, diperlukan prosedur deskriptif dengan menggunakan kunci yang sama. Oleh karena itu, kriptografi memungkinkan keamanan informasi melalui proses enkripsi dan deskripsi. Dengan passcode tersebut, Anda dapat menjaga privasi file penting Showroom Mobil Baroqah Anda. Cipher yang digunakan akan menggunakan metode "Advanced Encryption Standard" (AES-128). Metode "Advanced Encryption Standard (AES-128)" adalah algoritma enkripsi simetris yang banyak digunakan untuk mengamankan data di berbagai aplikasi dan protokol. Hasilnya adalah selama enkripsi dan dekripsi file, file tidak rusak sebelum dan sesudah enkripsi dan dekripsi. Metode yang digunakan dalam penelitian ini adalah black box messaging, yaitu metode troubleshooting dan pengujian fungsionalitas aplikasi berdasarkan input yang diterima dengan benar dan output yang dihasilkan sesuai dengan yang diharapkan. Hasil pencarian dengan metode pesan kotak hitam dengan data yang dicentang, jika tes tidak cocok, memberikan hasil yang salah, dan jika cocok, memberikan hasil yang valid. Proses pendataan dilakukan berdasarkan data penjualan dan pembelian di Showroom Mobil Baroqah.

Kata Kunci: Showroom Baroqah Mobil, Kriptografi, *Advanced Encryption Standard (AES-128), Plaintext, Chipertext*, Enkripsi dan Dekripsi.

CRYPTOGRAPHIC IMPLEMENTATION USING AES-128 TO SECURE SALES AND PURCHASE DATA ON BAROQAH MOBIL SHOWROOM

Abstract- *Baroqah Car Showroom is a long-established automotive trading company. To store sales, purchases, and other data, you need a data security app. This study used data collection methods, namely by making observations and surveys directly to the research location (observation), by conducting question and answer sessions directly to the resource persons (interviews) and by taking notes by reading the guidebook. The results showed that programs related to sales data security are needed for showrooms. So that data in the showroom is not lost or leaked, it is necessary to have an application or website to secure data. Cryptography is an information security technique that involves processing original information (clear text) using keys in the encryption process. This can generate a new message called ciphertext, which cannot be read directly. To return the ciphertext to its original information, a descriptive procedure using the same key is required. Therefore, cryptography allows information security through the process of encryption and description. With the passcode, you can maintain the privacy of your important Baroqah Car Showroom files. The cipher used will use the "Advanced Encryption Standard" (AES-128) method. The "Advanced Encryption Standard (AES-128)" method is a symmetric encryption algorithm that is widely used to secure data in various applications and protocols. The result is that during file encryption and decryption, files are not damaged before and after encryption and decryption. The method used in this study is black box messaging, which is a method of troubleshooting and testing application functionality based on input that is received correctly and the resulting output is as expected. Search results with the black box message method with checked data, if the test does not match, returns an incorrect result, and if it matches, a valid result. The data collection process was carried out based on sales and purchase data at the Baroqah Car Showroom.*

***Keywords**: Baroqah Car Showroom, Cryptography, Advanced Encryption Standard (AES-128), Plaintext, Chipertext, Encryption and Decryption.*

1. PENDAHULUAN

Showroom Baroqah Mobil merupakan suatu usaha jual-beli mobil bekas yang berlokasi di Lengkong Wetan, BSD Serpong Kota Tangerang Selatan. Dalam usaha *showroom* ini memiliki data penting seperti data penjualan dan data pembelian yang disimpan dalam format PDF. *Showroom* ini masih menyimpan data penjualan dan pembelian di dalam suatu folder tanpa adanya pengamanan data sehingga data tersebut tidak bisa dibilang aman. Oleh sebab itu, untuk menghindari atau mengantisipasi hal yang tidak diinginkan perlu adanya aplikasi yang bisa mengamankan data-data peting tersebut.

Saat menyadari pentingnya mengamankan data mereka, Showroom Baroqah Mobil telah memutuskan untuk mencari solusi yang efektif. Salah satu solusi yang mereka pertimbangkan adalah kriptografi. Kriptografi adalah ilmu dan teknik yang berkaitan dengan mengamankan komunikasi dan data dengan menggunakan algoritma dan kunci enkripsi. Dengan menerapkan kriptografi, Showroom Baroqah Mobil dapat melindungi data penjualan dan pembelian.

Tujuan utama kriptografi adalah untuk melindungi kerahasiaan, integritas dan keaslian data atau pesan yang dikirimkan melalui media apapun seperti komputer, jaringan komputer atau komunikasi elektronik. Untuk meminimalisir suatu kejadian atau hal-hal yang tidak diinginkan, dibutuhkan sebuah sistem keamanan data untuk melindungi data tersebut. Keamanan sistem ini disediakan oleh teknologi enkripsi *modern* menggunakan kata kunci sistem dan metode yang dipakai yaitu *Advanced Encryption Standard* (AES-128)[1].

Dengan menerapkan solusi kriptografi, Showroom Baroqah Mobil dapat melindungi data penjualan dan pembelian yang ada dalam format PDF dengan lebih baik. Ini akan membantu mengurangi risiko akses yang tidak sah, kebocoran data, atau modifikasi yang tidak diinginkan. Dalam prosesnya, solusi kriptografi akan memberikan lapisan keamanan dan membantu menjaga kepercayaan pelanggan serta reputasi showroom dalam menjaga kerahasiaan dan keamanan data mereka.

Advanced Encryption Standard (AES-128) adalah sebuah algoritma enkripsi simetris yang digunakan secara luas untuk melindungi data sensitif AES-128 menggunakan blok ukuran 128 bit dan kunci enkripsi dengan panjang 128 bit. Enkripsi AES-128 melibatkan serangkaian putaran penggantian, pergeseran, dan xor yang kompleks untuk mencampur dan mengacak data sebelum menghasilkan keluaran yang terenkripsi. Dalam proses perlindungan data, enkripsi terjadi, yaitu konversi data teks atau pesan (*plaintext*) menjadi data sandi (*ciphertext*), dan deskripsi mengubah data sandi (*ciphertext*) ke data awal (*plaintext*)[2].

AES dirancang agar dapat menggantikan algoritma sebelumnya, *Data Encryption Standard (DES)*, yang dianggap kurang aman dan kurang mampu menghadapi serangan modern. *National Institute of Standards and Technologi* (NIST) memilih AES sebagai standar pada tahun 2001 setelah melalui prosedur seleksi yang ketat [3].

Jenis enkripsi AES ini bergantung pada panjang kunci yang digunakan. Angka setelah istilah AES menjelaskan panjang kunci yang digunakan di setiap AES. Juga yang berbeda untuk setiap AES adalah jumlah putaran yang digunakan [4]. AES-128 menggunakan 10 putaran, AES-192 menggunakan 12 putaran, dan AES-256 menggunakan 14 putaran. Pada dasarnya AES menggunakan *block cipher* dengan panjang 128 bit dan mendukung kunci dengan panjang 128, 192 atau 256 bit. Algoritma tersebut menggabungkan beberapa transformasi matematis seperti penggantian *byte*, pertukaran baris, dan pemetaan ke matriks *Galois* untuk mengenkripsi dan mendekripsi data [5].

Penelitian sebelumnya yaitu "Pengamanan Data Pelanggan dan Penjual Menggunakan Implementasi Algoritma RSA" yang mengimplementasikan aplikasi berbasis *web* dan menggunakan metode RSA, sedangkan pada penelitian kali ini berbasis web untuk mengamankan data penjualan dan pembelian dengan menggunakan metode AES-128 [6].

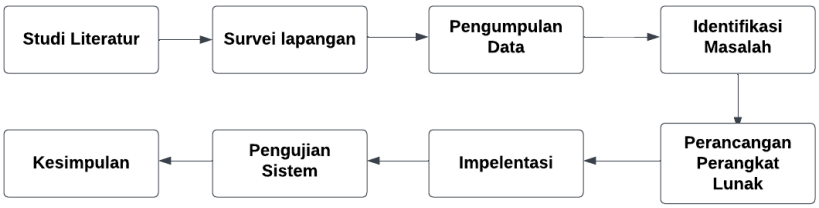
Penelitian yang menjadi rujukan yaitu "Impelentasi Algoritma AES-128 Pada Penjualan Alat-alat Elektronik berbasis *Web* (Studi Kasus Toko Sonia Elektronik)" yang mengimplementasikan aplikasi berbasis web dan menggunakan metode yang sama yaitu AES-128, maka dari itu merupakan rujukan penelitian [7].

Perbedaan penelitian yang menjadi rujukan dengan penelitian sebelumnya adalah metode algoritmanya saya, antara metode RSA dan AES-128 setelah melakukan perbandingan peneliti memilih metode AES-128 karena bisa disebut metode yang baru dan terkenal aman serta sekarang ini banyak yang menggunakan metode AES-128.

2. METODE PENELITIAN

A. *Flowchart* Penelitian

Metode waterfall adalah metode yang digunakan dalam penelitian ini dan merupakan prinsip dalam melakukan penelitian agar tidak terjadi penyimpangan, kesalahan dari hasil dan tujuan yang telah dicapai untuk penelitian yang lebih baik. Gambar 1 menyajikan *flowchart* penelitian.



Gambar 1. *Flowchart* Penelitian

B. Tahapan Pengumpulan Data

Wawancara (*Interview*). wawancara dengan pihak terkait yang bertujuan agar dapat mengantisipasi permasalahan yang sudah ada sehingga dapat menghasilkan sebuah perancangan sistem yang dapat menyelesaikan masalah tersebut. Observasi (*Observation*). Pada Showroom Baroqah Mobil untuk mengetahui keadaan sebenarnya dari objek penelitian. Tujuannya adalah untuk memperoleh penjelasan tentang informasi dan data yang diperlukan untuk penelitian.

C. Analisis sistem

1. Analisis Data

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

2. Menganalisis penerapan algoritma.

   Setelah tahap pengumpulan data dan memantau pengoperasian sistem. Selanjutnya, implementasi alias dari algoritma dilakukan. Analisis Aplikasi Algoritmik menjelaskan langkah-langkah penerapan enkripsi AES (Advanced Encryption Standard) untuk melindungi data penting. Begitu juga :

   A. Tentukan kunci yang akan digunakan untuk mengenkripsi dan mendekripsi file.
   B. Proses mengenkripsi file dengan kunci enkripsi, khususnya proses mengubah file terenkripsi menjadi ciphertext menggunakan kunci enkripsi.
   C. Proses dekripsi ciphertext menggunakan kunci yang sama dengan kunci enkripsi, yaitu proses mengubah ciphertext menjadi pesan yang dapat dibaca (plaintext).

3. Analisis sistem.

   Sistem menerapkan pengamanan melalui proses enkripsi konten file. Proses enkripsi dilaksanakan guna melindungi konten file yang bersifat rahasia, hanya dapat diakses oleh pihak yang memiliki otoritas. Implementasi ini memerlukan sebuah modul enkripsi yang terintegrasi dalam aplikasi, dan modul ini akan diaktifkan saat pengguna melakukan langkah pengamanan terhadap isi file. Sejauh ini, modul dekripsi baru diaktifkan ketika pengguna berkeinginan untuk menampilkan isi file tersebut..

D. 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.

E. 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 phpMyAdmin sebagai databasenya.
2. Hardware yang digunakan adalah MSI Modern 14 BSM, prosesor AMD Ryzen 5 5500U, RAM 16 GB DDR4, SSD 512 GB.

F. 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.

G. Kesimpulan

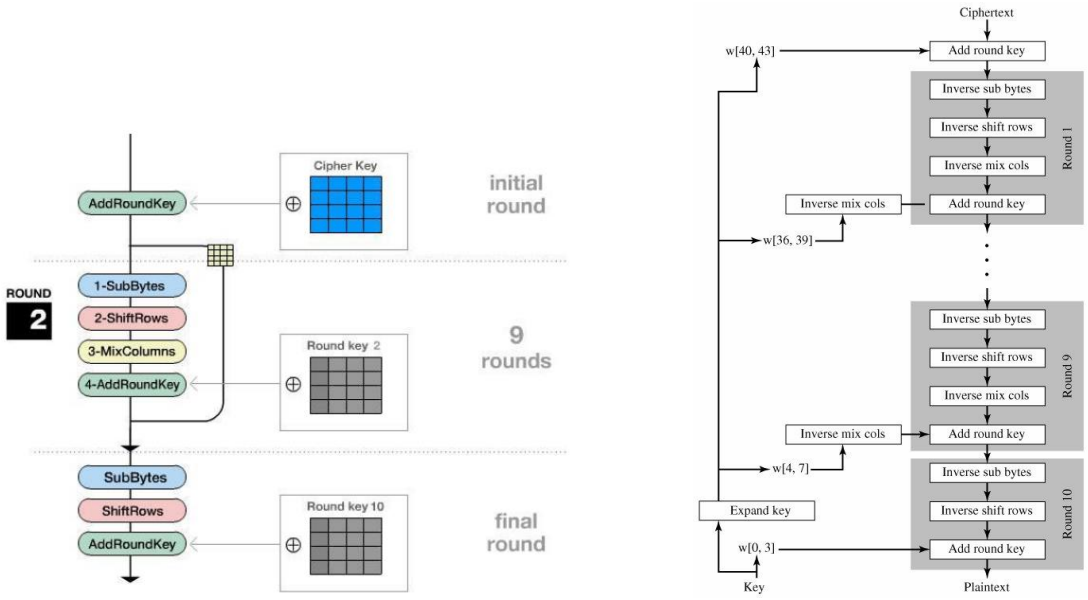
Tahap akhir ini menyimpulkan bahwa penerapan metode kriptografi *Advanced Encryption Standard* (AES) 128, berjalan dengan baik, dan dapat mengamankan file data yang dibeli dan dijual di Galeri Baroqah Mobil aman dan pada tahap ini, ada usulan pengembangan dalam sistem ini .

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 AES-128 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. [8].

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 [9]. Gambar 2 berikut menunjukkan proses enkripsi AES-128:

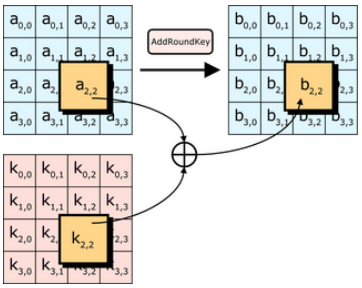


Gambar 2. Proses Enkripsi dan Dekripsi

Langkah kerja enkripsi sebagai berikut:

1. AddRoundKey

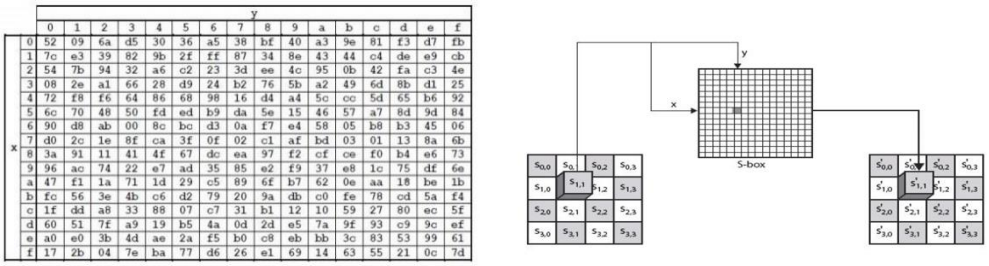
AddRoundKey merupakan sebuah Round Key yang ditambahkan pada state dengan operasi XOR. AddRoundKey pada dasarnya adalah mengkombinasi chiptertext dengan hubungan XOR [10]. Dapat dilihat pada gambar 3 berikut ini :



Gambar 3. AddRoundKey

2. SubBytes

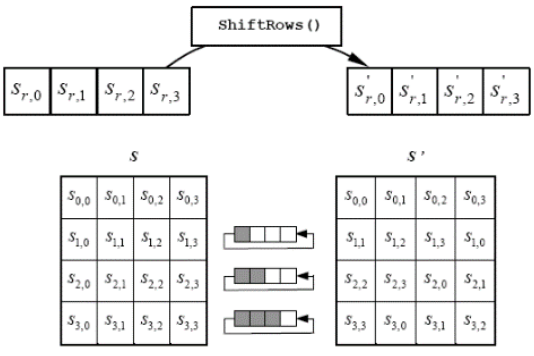
Prinsip dari *SubBytes* adalah mengganti isi matriks atau tabel yang telah ada dengan matriks atau tabel lain yang disebut dengan Rijndael S-Box [10]. Dapat dilihat pada gambar 4 merupakan contoh dari *SubBytes* dan Rijndael S-Box berikut ini :



Gambar 4. S-Box dan Ilustrasi *SubBytes*

3. ShiftRows

Seperti Namanya, *ShiftRows* merupakan metode yang melakukan *shift* atau pergeseran pada tiap elemen *blok* atau tabel dalam satu baris. Pada metode ini, baris pertama tidak dilakukan pergeseran, namun pada baris kedua dilakukan pergeseran 1 *byte*, baris ketiga dilakukan pergeseran 2 *byte*, dan seterusnya. Perubahan ini dapat dilihat pada *blok* yang merupakan pergeseran ke kiri setiap elemen tergantung berapa *byte* perubahannya, setiap perubahan 1 *byte* menunjukkan pergeseran ke kiri [10]. Dapat dilihat pada gambar 5 berikut ini :

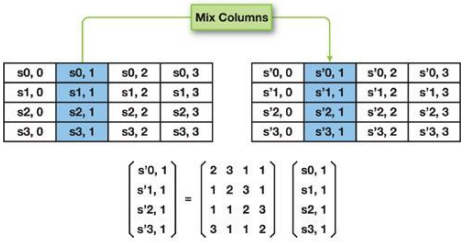


Gambar 5. *ShiftRows*

4. MixColumns

Apa yang terjadi ketika MixColumns adalah bahwa setiap elemen blok cipher dikalikan dengan matriks yang ditunjukkan pada gambar. Tabel didefinisikan dan siap untuk digunakan. Perkalian dilakukan dengan cara yang sama seperti perkalian matriks biasa, yaitu menggunakan dot product, kemudian kedua perkalian tersebut dimasukkan ke dalam blok cipher yang baru. Contoh pada gambar ini akan menjelaskan cara melakukan perkalian ini. Oleh karena itu, seluruh rangkaian proses yang berlangsung dalam AES telah dijelaskan, dan langkah

selanjutnya adalah menjelaskan penggunaan masing-masing proses tersebut [10]. Dapat dilihat pada gambar 6 berikut ini :



Gambar 6. *MixColumns*

5. Key Expencion

Algoritma AES mengambil *chipper key* yang disediakan oleh pengguna dan memanggil fungsi *KeyExpansion* untuk menghasilkan beberapa *RoundKey* (jumlah *RoundKey* tergantung pada jumlah *round*) [10].

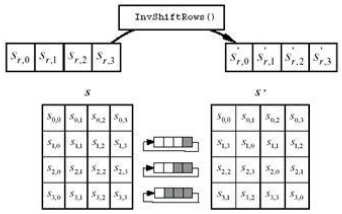
2.3 Proses Dekripsi

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. 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 [11]. Proses dekripsi AES-128 dapat dilihat pada gambar 2. berikut:

Langkah kerja dekripsi adalah sebagai berikut :

A. *InversShiftRows.*

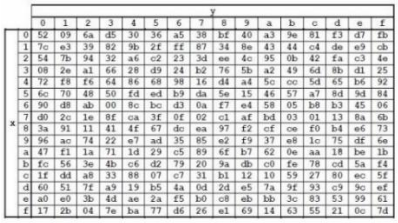
InversShiftRows merupakan transformasi *byte* yang dibalikan dengan transformasi *ShiftRows*. Pada transformasi *InversShiftRows*, dilakukan pergeseran antara bit ke kanan sedangkan pada *ShiftRows*, dilakukan pergeseran bit ke kiri [12]. Contoh transformasi *InversShiftRows* terdapat pada gambar 7 berikut ini :



Gambar 7. Proses *InversShiftRows*

B. *InversSubBytes*

InversSubByte merupakan transformasi *byte* yang berbanding terbalik dengan transformasi *SubBytes*. Pada *InversSubByte*, tiap elemen S-BOX [12]. Terdapat pada gambar 8 berikut ini:



x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Gambar 8. *InverSubBytes* elemen S-Box

C. *InversMixColumns*

Setelah *InversSubBytes* proses selajutnya yaitu *InversMixColumns* pada proses ini tiap kolom dalam *state* dikalikan dengan matriks perkalian dalam *Advance Encryption Standard* (AES) [12]. Perkalian dalam bentuk matriks dapat ditulis sebagai berikut:

$$\begin{pmatrix} S'\ 0,c \\ S'\ 1,c \\ S'\ 2,c \\ S'\ 3,c \end{pmatrix} = \begin{pmatrix} 0E\ 0B\ 0D\ \Theta \\ \Theta\ \ 0E\ 0B\ OD \\ 0D\ \Theta\ OE\ OB \\ 0B\ OD\ \Theta\ OE \end{pmatrix} \begin{pmatrix} S\ 0,c \\ S\ 1,c \\ S\ 2,c \\ S\ 3,c \end{pmatrix}$$

Hasil dari perkalian matriks adalah

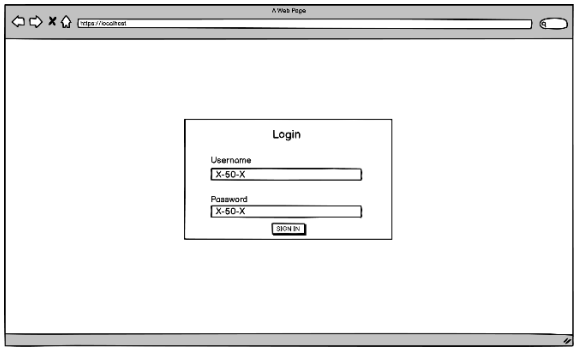
S' 0,c = ({0E} ● S 0,c) ({0B}⊕● S1,c) ({0D}⊕● S2,c) ({Θ}⊕ S3,c)
S' 1,c = ({Θ} ● S 0,c) ({0E}⊕ S1,c) ({0B}⊕ S2,c) ({0D}⊕● S3,c)
S' 1,c = ({0D} ● S 0,c) ({Θ} ⊕S1,c) ({0E}⊕ S2,c) ({0B}⊕ S3,c)
S' 1,c = ({0B} ● S 0,c) ({0D}⊕ S1,c) ({Θ}⊕S2,c) ({0E} ⊕S3,c)

D. *InversAddRoundKey*

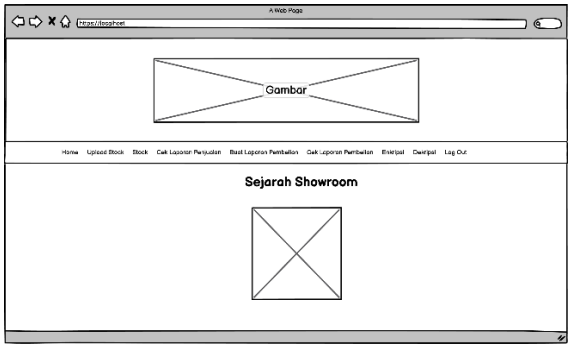
Transformaasi *InversAddRoundKey* sama dengan transformasi *AddRoundKey* karena dalam transformasi ini hanya dilakukan operasi penambahan sederhana dengan operasi *bitwise* XOR [12].

2.4 Rancangan Layar

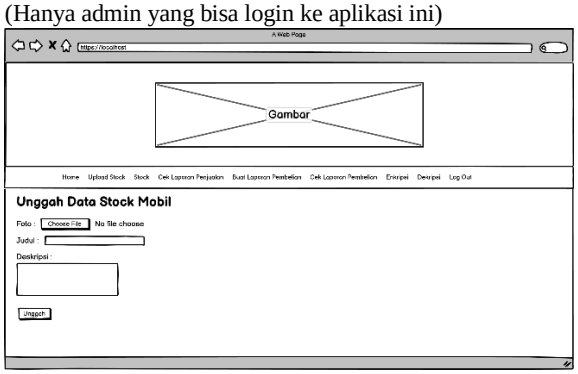
Saat membuat aplikasi, sangat penting untuk mendesain bagian layar sebagai bentuk dasar untuk membuat desain aplikasi yang diinginkan. Desain layar harus mudah dipahami, tujuannya agar pengguna merasa nyaman dan tidak bingung saat menggunakan aplikasi ini [13]. Dapat dilihat pada gambar 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 berikut:



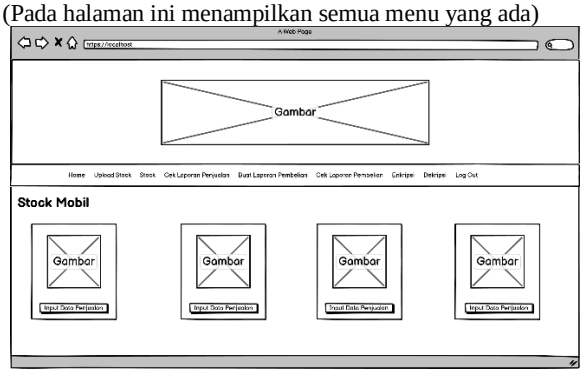
Gambar 9. Rancangan Layar *Login*
(Hanya admin yang bisa login ke aplikasi ini)



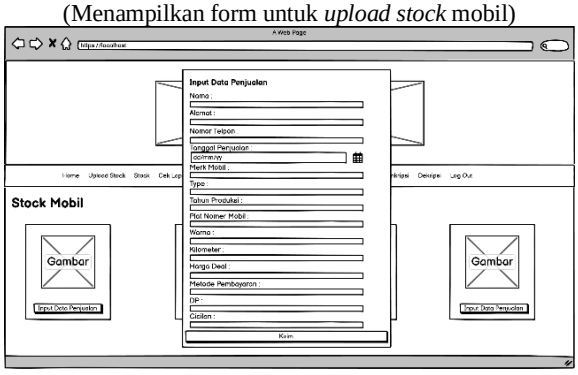
Gambar 10. Rancangan Layar *Home*
(Pada halaman ini menampilkan semua menu yang ada)



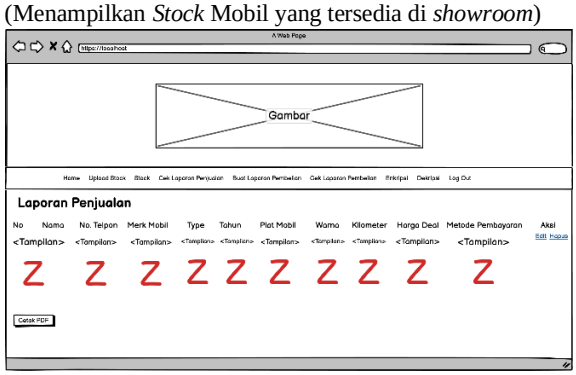
Gambar 11. Rancangan Layar *Upload Stock*
(Menampilkan form untuk *upload stock* mobil)



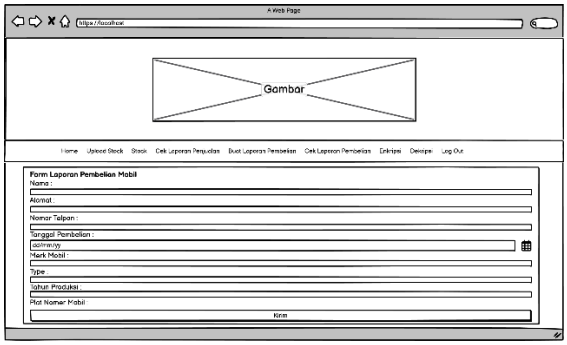
Gambar 12. Rancangan Layar *Stock* Mobil
(Menampilkan *Stock* Mobil yang tersedia di *showroom*)



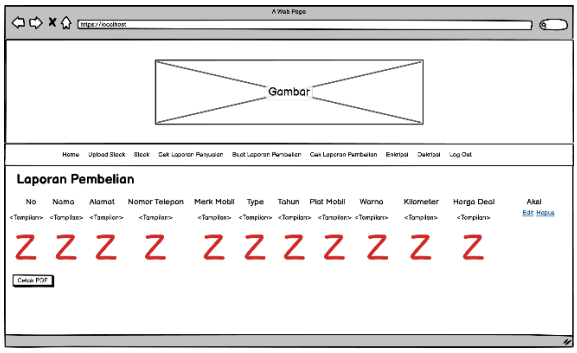
Gambar 13. Rancangan Layar Input Data Penjualan
(Menampilkan form untuk input data penjualan).



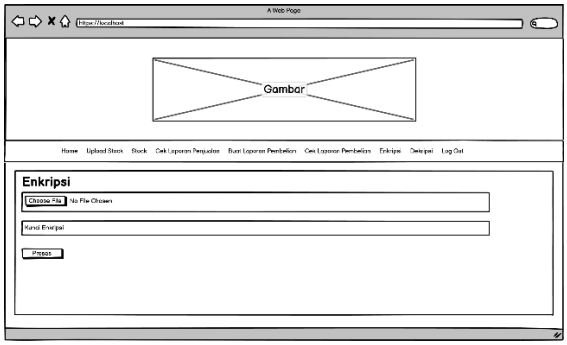
Gambar 14. Rancangan Layar Laporan Penjualan
(Menampilkan data hasil inputan dari input data penjualan)



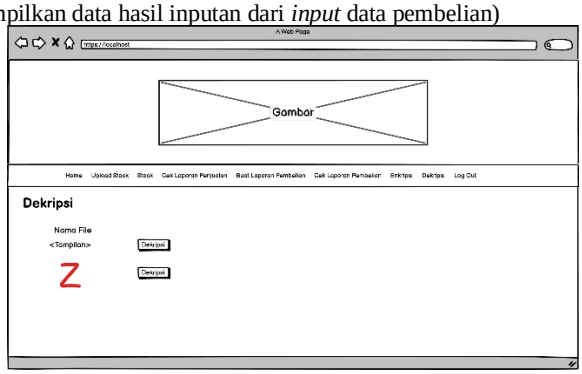
Gambar 15. Rancangan Layar *Input* Data Pembelian | (Menampilkan *form* untuk *input* data pembelian)



Gambar 16. Rancangan Layar Laporan Pembelian | (Menampilkan data hasil inputan dari *input* data pembelian)



Gambar 17. Rancangan Layar Enkripsi *File*
(Menampilkan *form* untuk pilih *file* dan *input key*)



Gambar 18. Rancangan Layar Dekripsi *File*
(Menampilkan file yang akan di dekripsi dan prosesnya)

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

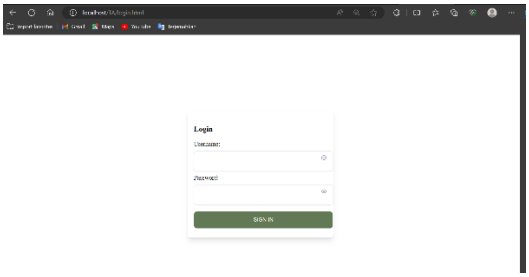
Flowchart Menu Enkripsi merupakan *flowchart* dari halaman *form* enkripsi, dimana *flowchart* ini menjelaskan tentang melakukan enkripsi file, dalam mengenkripsi file admin harus memasukkan *password*, setelah itu program akan memproses enkripsi.

3.2 *Flowchart* Menu Dekripsi

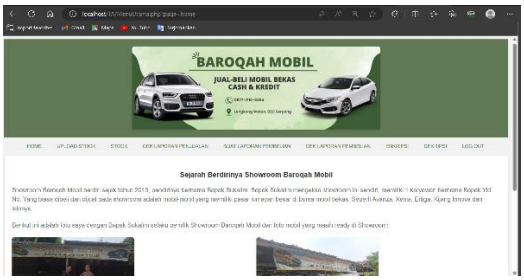
Flowchart Menu Dekripsi merupakan *flowchart* dari halaman dekripsi, dimana *flowchart* ini menjelaskan tentang melakukan dekripsi file. Dalam dekripsi file admin harus memasukkan *password* yang sesuai dengan enkripsi, setelah itu program akan memproses dekripsi.

3.3 Tampilan Layar

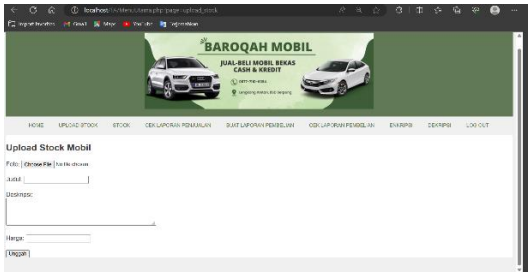
Pada gambar 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 terdapat tampilan layar aplikasi pengamanan data *showroom* baik dari menu *login* hingga menu *log out*. Sebagai berikut tampilan layar aplikasi pengamanan data *showroom*.



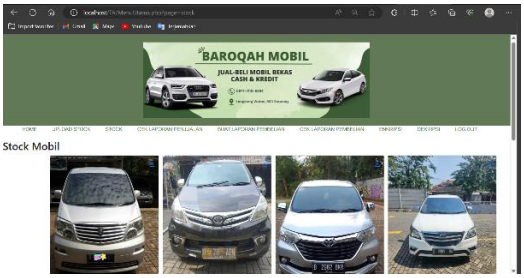
Gambar 19. Tampilan Layar *Login*
(Hanya admin yang bisa login ke aplikasi ini)



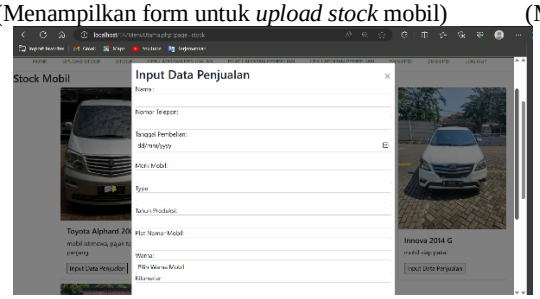
Gambar 20. Tampilan Layar *Home*
(Pada halaman ini menampilkan semua menu yang ada)



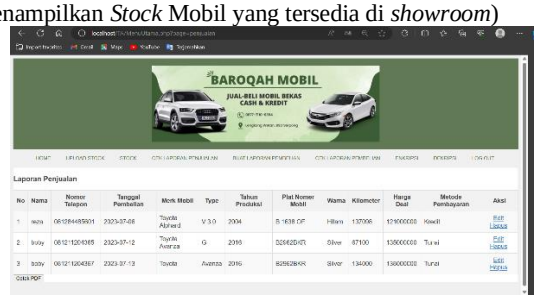
Gambar 21. Tampilan Layar *Upload Stock* (Menampilkan form untuk *upload stock* mobil)



Gambar 22. Tampilan Layar *Stock* Mobil (Menampilkan *Stock* Mobil yang tersedia di *showroom*)

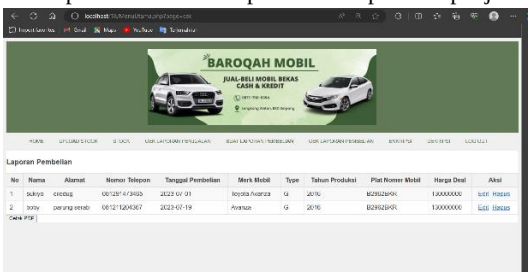


Gambar 23. Tampilan Layar Input Data Penjualan (Menampilkan form untuk input data penjualan).



Gambar 24. Tampilan Layar Laporan Penjualan (Menampilkan data hasil inputan dari input data penjualan)

Gambar 25. Tampilan Layar *Input* Data Pembelian (Menampilkan *form* untuk *input* data pembelian)



Gambar 26. Tampilan Layar Laporan Pembelian (Menampilkan data hasil inputan dari *input* data pembelian)

Gambar 27. Tampilan Layar Enkripsi *File* (Menampilkan *form* untuk pilih *file* dan *input key*)

Gambar 28. Tampilan Layar Dekripsi *File* (Menampilkan file yang akan di dekripsi dan prosesnya)

3.4 Pengujian

Dari pengujian yang dilakukan, terdapat aspek kecepatan dan hasil enkripsi berupa file yang tidak dapat dibuka dan beberapa ukuran data sebelum dan sesudah dienkripsi dengan algoritma enkripsi AES-128. Tabel 1 menunjukkan hasil pengujian yang dilakukan.

Tabel 1. Hasil Pengujian Enkripsi dan Dekripsi File

Nama File	Ukuran File (*Kilobyte*)			Waktu (Detik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
Sejarah Showroom.pdf	33kb	44kb	33kb	1,31 detik	1,27 detik
Nim.docx	12kb	16kb	12kb	0,20 detik	0,18 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 Baroqah Mobil. Dengan memodifikasi proses enkripsi khususnya pada *random key*, aplikasi ini memiliki tingkat keamanan yang tinggi. Aplikasi ini bisa mengamankan *file* dengan format *.pdf, .docx, .xlsx*.

Diharapkan untuk dikembangkan lagi untuk program enkripsi dan dekripsi file ini dengan memodifikasi ataupu 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] I. Dian Widyawan, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Knkt", *Skanika* Vol. 4, No. 1, Pp. 15–22, 2021.
[2] 2016, B. Cyber, Klinik Informatika. Available: Https://Klinikinformatikacyber.Blogspot.Com/2016/03/Pengertian-Dan-Sistem-Kerja-Aes-Iii.Html
[3] 2021, B. Pasogit, Studentterpelajar. Available: Https://Www.Studentterpelajar.Com/2021/03/Pengertian-Algoritma-Aes.Html.
[4] 2018, B.B. Fze, Ukdiss.Com. Available: Https://Ukdiss.Com/Examples/Cryptography-Methods-Data-Security.Php?Vref=1.
[5] I. Gunawan, "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi Aes Dari Serangan Brute Force", Techsi-Jurnal Teknik Informatika, 13(1), 14-25.
[6] K. Adriani & H. B. Hayadi, "Pengamanan Data Penjualan Dengan Kriptografi Algoritma Rivest Shamir Adleman (Rsa) Pada Toko Baju Family", *Journal Of Science And Social Research*, Vol.4 Pp. 664-670. 2022
[7] H. Wulandari, J. Karman & Elmayanti, "Impelentasi Algoritma Aes-128 Pada Penjualan Alat-Alat Elektronik Berbasis Web (Studi Kasus Toko Sonia Elektronik)", *Jurnal Teknologi Informasi Muara*, Vol.15, Pp.1-11, 2023.
[8] 2023, Admin, P3mpbc.Uma.Ac.Id. Available: Https://P3mpbc.Uma.Ac.Id/2023/01/07/Perbedaan-Simetris-Dan-Asimetris-Pada-Kriptografi/.
[9] Hamid Wijaya, "Implementasi Kriptografi Aes-128 Untuk Mengamankan Url (Uniform Resource Locator) Dari Sql Injection". *Jurnal Akademika* Vol.3, Pp. 1-8, 2020.
[10] G. Grehasen & S. Mulyati, "Pengamanan Database Pada Aplikasi Test Masuk Karyawan Baru Berbasis Web Menggunakan Algoritma Kriptografi Aes-128 Dan Rc4", Journal.Budiluhur.Ac.Id Vol.14, Pp. 1-9, 2017.
[11] Munir, Rinaldi. "Pengantar Kriptografi". Itb Bandung: Penerbit Informatika.
[12] R. Rahmawati & D. Rahardjo, "Aplikasi Pengamanan Data Menggunakan Algoritme Steganografi Discrete Cosine Transform Dan Kriptografi Aes 128 Bit Pada Smk Pgri 16 Jakarta", *Jurnal Teknik Informatika Dan Sistem Informasi*, 67-73.
[13] 2021, G. Istia, Scribd. Available: Https//Www.Scribd.Com/Document/507369841/Imk#.