Implementasi *Advanced Encryption Standard 128* Sebagai Pengamanan Basis Data Obat-obatan Apotek

http://dx.doi.org/10.28932/jutisi.v8i2.4817

Riwayat Artikel
Received: 17 Mei 2022 | *Final Revision*: 3 Agustus 2022 | *Accepted*: 5 Agustus 2022

Yudi Wiharto[✉ #1], Mufti[*2]

[#] *Program studi Teknik Informatika, Universitas Budi Luhur*
Jl. Ciledug Raya, Petukangan Utara, Kota Jakarta Selatan, 12260, Indonesia
[1]yudi.wiharto@budiluhur.ac.id
[2]mufti@budiluhur.ac.id
✉Corresponding author: yudi.wiharto@budiluhur.ac.id

Abstrak — **Kerahasiaan dan keamanan data merupakan dua hal penting dalam komunikasi data sebagai upaya menjaga kerahasiaan dan keamanan suatu data, sehingga penelitian ini bertujuan untuk membuat suatu sistem yang digunakan untuk meningkatkan kerahasiaan dan keamanan data obat di apotek dengan menggunakan Advanced Encryption Standar 128, dimana Algoritma kriptografi Advanced Encryption Standard (AES-128) sebagai metode yang akan digunakan. Pengujian enkripsi dilakukan dengan melakukan perbandingan antara perhitungan manual dengan hasil enkripsi pada sistem. Pembuatan sistem ini dilakukan dengan mengumpulkan data, merancang sistem dengan database. Hasil dari pembuatan sistem adalah aplikasi berbasis web yang digunakan dalam kegiatan apoteker atau pegawai apotek untuk menginput dan mengelola data obat.**

Kata kunci— **AES-128; Algoritma; Data; Kriptografi; Sistem.**

Implementation of Advanced Encryption Standard 128 to Secure Pharmacy Drug Database

Abstract — ***Confidentiality and data security are two important things in data communication as an effort to maintain the confidentiality and security of data, so this study aims to create a system that is used to improve the confidentiality and security of drug data in pharmacies by using Advanced Encryption Standard 128, where the cryptographic algorithm Advanced Encryption Standard (AES-128) as the method to be used. Encryption testing is done by comparing manual calculations with the results of encryption on the system. Making this system is done by collecting data, designing a system with a database. The result of making the system is a web-based application that is used in the activities of pharmacists or pharmacy employees to input and manage drug data.***

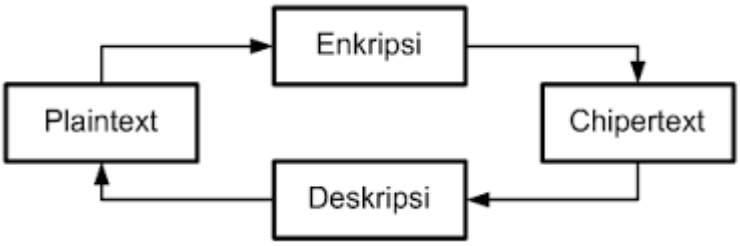
Keywords— ***AES-128; Algorithm; Cryptography; Data; System.***

I. PENDAHULUAN

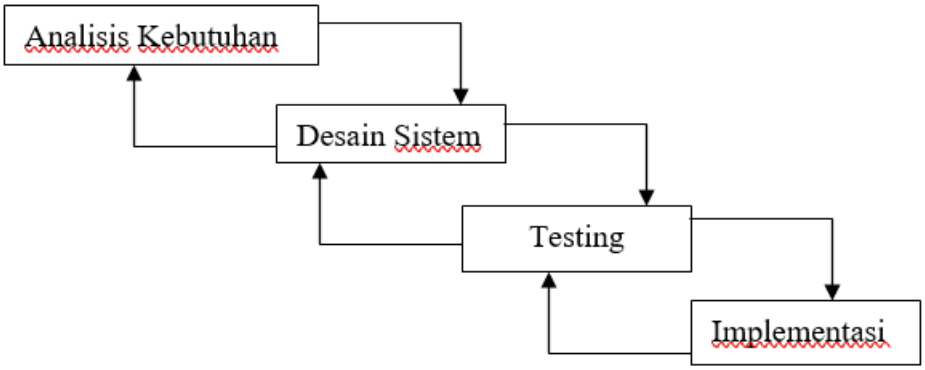
Permasalahan kerahasiaan data yang terjadi pada sebuah Apotek yaitu, pada saat proses input data obat-obatan yang tersedia mempunyai informasi seperti harga asli, jenis obat, fungsi obat yang nantinya akan disimpan ke dalam komputer, tersimpan secara terbuka tanpa adanya pengamanan data dimana semua pegawai dan staff dapat melihat data pada Apotek secara langsung tanpa dirahasiakan. Masalah keamanan dan kerahasian data ialah suatu hal yang sangat penting, untuk itu perlu dilakukan perlindungan terhadap data yang kita miliki [1]. Sebuah file dokumen seharusnya dijaga kerahasiaannya agar tidak disalahgunakan oleh orang yang tidak berhak [2]. Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama informasi sensitif yang hanya boleh diketahui oleh pihak yang berhak saja [3]. Kriptografi AES 128 bit memiliki ruang kunci 2^{128} yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan sehingga terhindar dari *brute force attack* [4]. Hasil pengujian menunjukkan bahwa nilai dari Algoritma AES berkisar antara 45-60%, dengan nilai tersebut akan membuat perbedaan yang cukup sulit untuk kriptanalis melakukan serangan [5]. Dengan aplikasi yang menggunakan kriptografi AES user bisa berkomunikasi aman tidak cemas pesannya dimanipulasi [6]. Pada kriptografi dikenal Algoritma *blockchiper* yang didalamnya terdapat AES (*Advanced Encryption Standard*) bagian dari *Modern Symmetric KeyCipher*, Algoritma ini menggunakan kunci sama disaat tahap enkripsi deskripsi sehingga data jadi sulit dipahami [7]. *Advanced Encryption Standard*, merupakan metode penyandian (mengubah teks asli menjadi teks tersandi) data dalam empat langkah dasar yaitu, langkah *nonlinear* (*Sub Bytes*), langkah dispersi (*Shit Rows*), langkah difusi (*Mix Columns*), dan penambahan kunci (*Add RoundKey*) [8]. Algoritma AES merupakan Algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi [9]. Enkripsi AES menunjukkan bahwa pesan yang sama dengan kunci yang berbeda dapat menghasilkan *chipertext* yang berbeda [10]. Kriptografi telah banyak diimplementasikan di banyak hal, Smart card, Anjungan Tunai Mandiri (ATM), Pay TV, Mobile Phone, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya [11]. Salah satu dampak negatif dalam perkembangan teknologi ialah adanya penyadapan data, yang merupakan salah satu masalah yang paling ditakuti oleh para pengguna jaringan komunikasi, karena itulah dibutuhkan suatu metode yang dapat menjaga kerahasiaan informasi ini, metode yang dimaksud ialah kriptografi, dalam perkembangannya kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dan tanda tangan digital dan keaslian pesan dengan sidik jari digital, secara umum kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita [12]. Oleh karena itu masalah yang dihadapi untuk keamanan suatu data merupakan aspek yang sangat penting. Pendataan pada Apotek baik Nama Obat, Berat, Harga dan Jenis Obat bersifat sangat penting, karena data tersebut begitu rentan dan bersifat penting bagi Apotek maka harus diberikan keamanan yang sangat baik, agar tidak mudah dimengerti mengenai data tersebut oleh pihak yang berniat buruk. Dari permasalahan yang dihadapi oleh Apotek, maka dibuat Aplikasi dengan pengamanan basis data menggunakan Algoritma Kriptografi *Advance Encryption Standard* (AES-128) berbasis Web untuk mengamankan seluruh data yang berkaitan dengan Apotek. Dengan aplikasi pengamanan basis data tersebut memiliki keamanan ganda selain terdapat username, password ada data yang terenkripsi juga. 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

II. METODE PENELITIAN

Tahap studi pustaka dilaksanakan dengan mengumpulkan data serta mempelajari semua yang terkait dengan ilmu kriptografi, Algoritma *AES 128* dan semua perihal terkait. Bagan alur konsep dasar enkripsi deskripsi dapat dilihat pada gambar 1 serta bagan dari tahapan metode *waterfall* dapat dilihat pada gambar 2.



Gambar 1. Konsep Dasar Enkripsi Dekripsi



Gambar 2. Metode *Waterfall*

1. *Analisis Kebutuhan*
   Teknologi informasi serta komunikasi menjadi kebutuhan pada semua bidang pekerjaan dan berkembang dengan sangat pesat, sehingga membutuhkan sebuah aplikasi dengan sistem tingkat keamanan yang baik agar bisa menjaga kerahasian data yang didalamnya terdapat proses enkripsi dekripsi dengan metode Algoritma AES
2. *Rancang Sistem*
   Proses desain sebuah aplikasi dengan sistem terbentuk dari dasar Analisa yang dibutuhkan. Sistem aplikasiini dapat melakukan enkripsi saat *user* melakukan simpan data. Perencanaan aplikasi menggunakan bahasa pemrograman PHP.
3. *Testing*
   Tahap ini, ialah proses pengujian aplikasi dan evaluasi kebutuhan sesuai pengguna.
4. *Implementasi*
   Pada tahap ini, proses penerapan sistem dilakukan sesuai hasil dari tahap pengujian dan evaluasi.

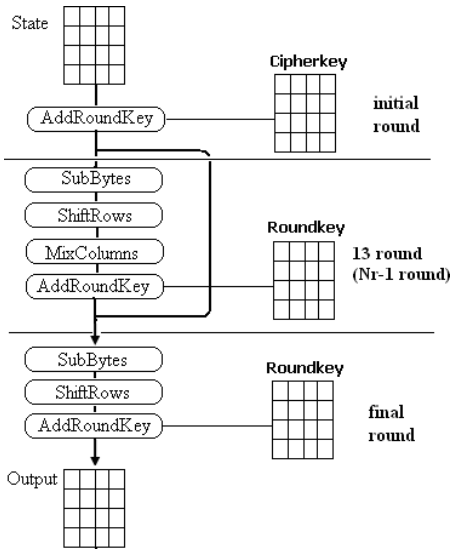
III. HASIL DAN PEMBAHASAN

A. Analisis Kebutuhan

Kriptografi dikenal juga sebagai Algoritma *blockchiper* didalamnya ada AES (*Advanced Encryption Standart*) yang di dalamnya ada *Modern Symmetric KeyCipher*, Algoritma memakai kunci sama dengan disaat tahapan enkripsi dekripsi hingga data jadi susah dipahami. Teknik Algoritma ini dipakai untuk konversi data dengan bentuk *character* acak dengan harapan data yang tersimpan tidak dapat dipahami oleh pihak lain yang tidak berwenang. Maka dari itu, sistem dengan keamanan data dibutuhkan agar kerahasian data dan informasi terjaga. Pembuatan aplikasi sistem dengan keamanan basis data ini berbasis web.

B. Tahap Enkripsi

Tahap enkripsi Algoritma AES sendiri memiliki 4 macam perubahan bytes, yaitu *Sub Bytes, Shift Rows, Mix columns*, dan *Add RoundKey*s. Di tahap pertama enkripsi, masukan yang sudah disalin pada state akan melakukan perubahan byte *Add RoundKey*. Lalu, state melakukan perubahan *Sub Bytes, Shift Rows, Mix Columns*, dan *Add RoundKey* dengan berulang kali sebanyak Nr. Tahap pada Algoritma AES biasa disebut dengan *round function*. Dimana *Round* terakhir sedikit beda dengan sebelumnya dimana saat *round* terakhir, *state* tidak melakukan perubahan *Mix Columns*. Gambaran tahap enkripsi AES bisa dilihat pada gambar 3.



Gambar 3. Bagan enkripsi AES-128

Algoritma AES yang beroperasi diblok 128-bit dengan kuncinya 128bit, diluar tahap menaikan *round key* adalah seperti dibawah ini:

1. *Add RoundKey*, menggunakan XOR di awal dengan *cipherkeys*.
2. *Runing* berulang Nr-1 kali. Tahap ini dijalankan di setiap putaran adalah :
   a. *Sub Bytes* adalah subtitusi *byte* dengan tabel S-Box.
   b. *Shift Rows* adalah pergeseran baris baris array distate.
   c. *Mix Columns* adalah tahap acak data di masing-masing kolom *array state*.
   d. *Add RoundKey* ialah menggunakan XOR pada state sekarang *roundkey*.
3. Round akhir, tahap putaran akhir :
   a. Sub Byte
   b. Shift Row
   c. Add RoundKey

Tahapan enkripsi seperti berikut:

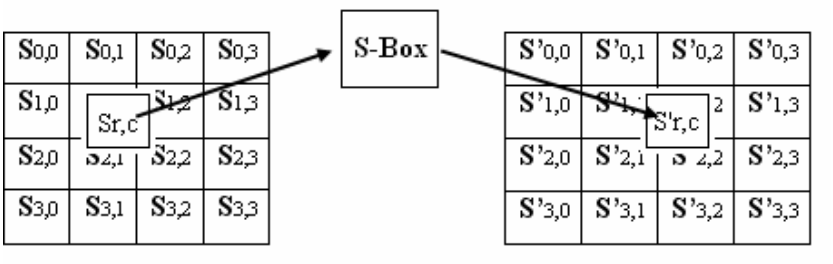
a. Perubahan Sub Bytes

Sub Bytes adalah perubahan byte dimana setiap data state dapat dimapkan dengan penggunaan tabel S-Box, seperti gambar 4.

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

Gambar 4. S-BOX

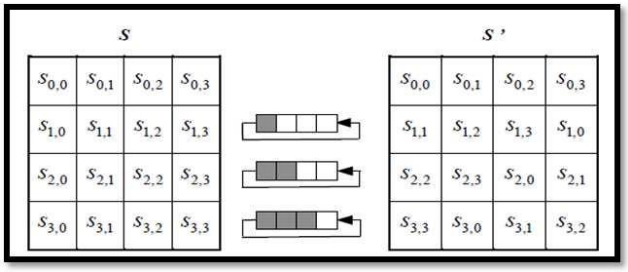
Untuk disetiap byte array distatet, misal S[r, c]=xy, diman xy ialah digit berupa heksadesimal nilai S [r,c], nilainya, ialah S'[r,c], ialah data didalam tabel subsitusi ini adalah potongan baris x dengan kolom y. Gambar 5 menampilkan pencocokan disetiap byte pada state.



Gambar 5. Pencocokan di setiap Byte pada state

b. Shiftrows

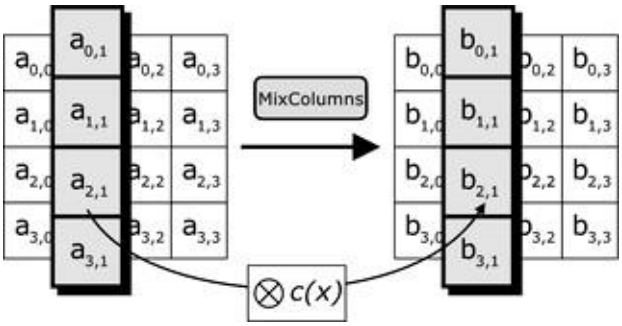
Perubahan *Shiftrows* sebenarnya ialah tahap pergerakan bit, dimana bit pojok kiri dipindahkan ke bit pojok kanan. Tahap pergerakan *Shiftrow* ditunjukkan pada gambar 6.



Gambar 6. Tahap shiftrows

c. Mix Columns

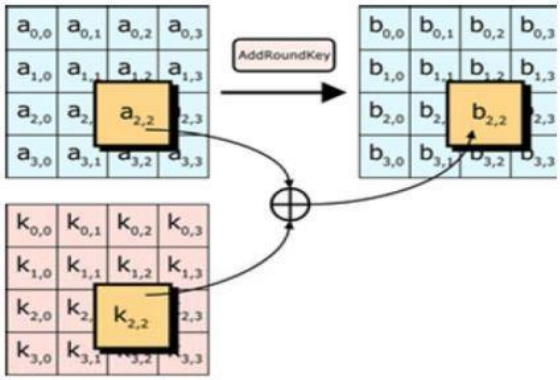
Mix Columns memproses setiap data pada satu kolom di state. Perubahan *mix columns* bisa dilihat pada gambar 7.



Gambar 7. Tahap mix columns

d. Add RoundKey

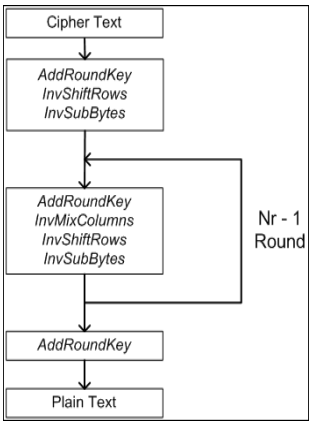
Add RoundKey: menggunakan XOR di antara state dengan *roundkey*. Dapat dilihat pada gambar 8.



Gambar 8. Tahap *Add RoundKey*

C. Tahap Dekripsi

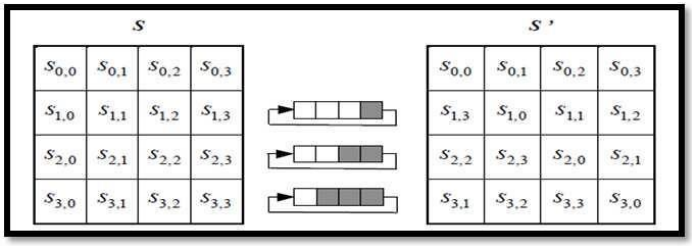
Tahap cipher bisa dibalikkan dengan diimplementasikan kedalam arah berlawanan agar mengeluarkan inverse cipher yang mudah dimengerti Algoritma AES. Perubahan *byte* yang dipakai dalam *inverse cipher* adalah *Inv Shift Rows, Inv Sub Bytes, InvMix Columns*, dan *Add RoundKey*. Tahap dekripsi bisa dilihat pada gambar 9.



Gambar 9. Tahap dekripsi

a. Inv Shiftrows

Inv *Shiftrows* ialah perubahan byte dengan kebalikan dari perubahan *Shift Rows*. Pada perubahan Inv *Shiftrows*, dilakukan geseran bit mengarah kanan sedangkan di *Shift Rows* dilakukan geseran bit mengarah kiri. Ilustrasi perubahan *Inv Shift Rows* dapat dilihat pada gambar 10.



Gambar 10. Tahap inv shift rows

b. Inv Sub Bytes

Inv Sub Bytes ialah perubahan bytes yang kebalikan dari perubahan SubBytes. Pada *Inv Sub Bytes*, tiap data di state di petakan dengan gambar 11.

Hex		Y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
X	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	17	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 11. Tahap invsubbytes

c. Inv Mix Columns

Di setiap kolom pada state akan dilakukan perkalian matrik pada AES. Tahap perkalian matrik bisa dilihat seperti dibawah ini :

$$\begin{bmatrix} S'_{0,C} \\ S'_{1,C} \\ S'_{2,C} \\ S'_{3,C} \end{bmatrix} = \begin{bmatrix} 0E\ 0B\ 0D\ \theta \\ \theta\ 0E\ 0B\ 0D \\ 0D\ \theta\ 0E\ 0B \\ 0B\ 0D\ \theta\ 0E \end{bmatrix} \begin{bmatrix} S_{0,C} \\ S_{1,C} \\ S_{2,C} \\ S_{3,C} \end{bmatrix}$$

Hasil perkalian matriksnya adalah:

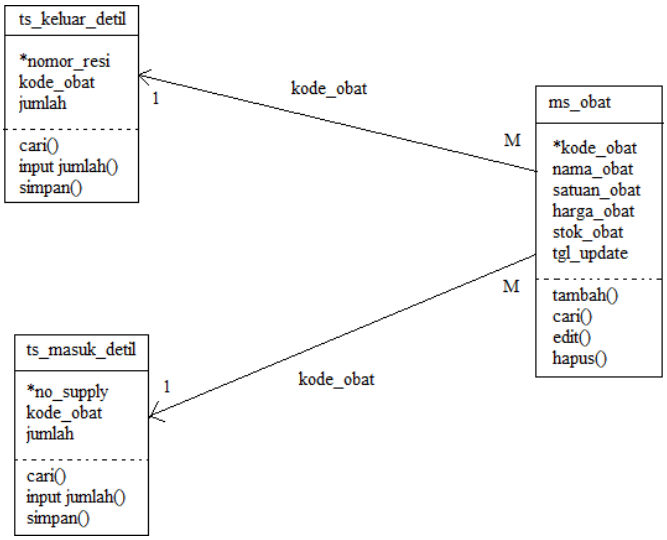
$$S'_{0,C} = (\{0E\} \bullet S_{0,C}) \oplus (\{0B\} \bullet S_{1,C}) \oplus (\{0D\} \bullet S_{2,C}) \oplus (\{\theta\} \bullet S_{3,C})$$
$$S'_{1,C} = (\{\theta\} \bullet S_{0,C}) \oplus (\{0E\} \bullet S_{1,C}) \oplus (\{0B\} \bullet S_{2,C}) \oplus (\{0D\} \bullet S_{3,C})$$
$$S'_{2,C} = (\{0D\} \bullet S_{0,C}) \oplus (\{\theta\} \bullet S_{1,C}) \oplus (\{0E\} \bullet S_{2,C}) \oplus (\{0B\} \bullet S_{3,C})$$
$$S'_{3,C} = (\{0B\} \bullet S_{0,C}) \oplus (\{0D\} \bullet S_{1,C}) \oplus (\{\theta\} \bullet S_{2,C}) \oplus (\{0E\} \bullet S_{3,C})$$

d. Inverse Add RounKey

Perubahan *Inverse Add RoundKey* tidak beda pada perubahan *AddRoundkey* karena pada perubahan ini hanya dioperasikan penambahan sederhana pada proses operasi *bitwiseXOR.*

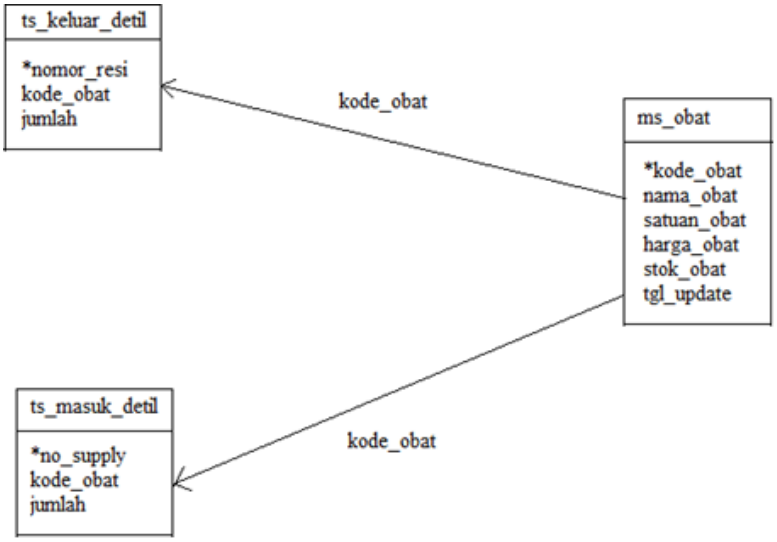
D. Rancangan Basis Data

Rancangan basis data ini digambarkan dengan *Class Diagram* dan *Logical Record Structure* (LRS). *Class Diagram* ini ilustrasi dari struktur dan hubungan antara objek-objek yang ada dalam aplikasi. Pada struktur ini meliputi metode dan atribut-atribut pada bagian-bagian *class*. Relasi pada masing-masing *class* ditunjukan pada gambar 12.



Gambar 12. Bagan Class Diagram

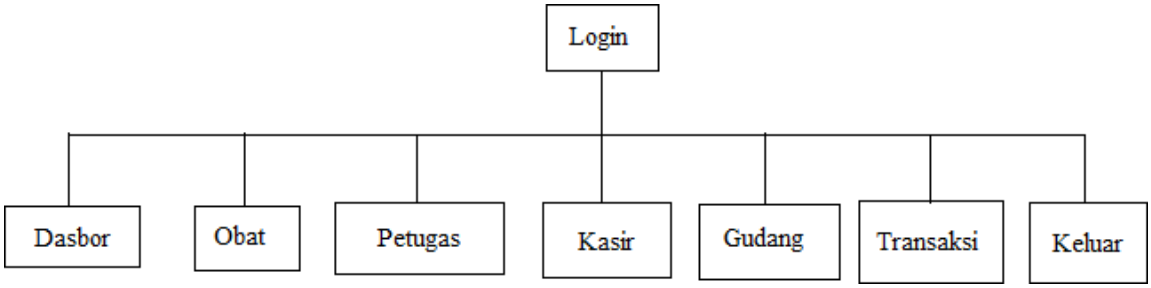
Bagan *Logical Record Structure* (LRS) sistem yang dibuat seperti gambar 13.



Gambar 13. Logical Record Structure (LRS)

E. Rancangan Menu

Struktur dari rancangan menu aplikasi ini menampilkan struktur kombinasi, karena menu yang ada saling berhubungan dengan menu utama dan sub menu yang tersedia sehingga *user* bisa berinteraksi lebih baik dengan menggunakan *cursor* untuk eksplorasi pada layer tampilan. Adapun gambar 14 sebagai rancangan menu dari aplikasi.



Gambar 14. Rancangan Menu

Aplikasi ini menggunakan pengamanan Basis Data dengan Algoritma *Advanced Encryption Standard* (AES-128) pada Apotek berjalan baik, spesifikasi yang direkomendasikan untuk diimplementasikan aplikasi ini di antaranya :

Perangkat Keras

1. Processor AMD Ryzen 5
2. RAM 8 GB
3. PC / Laptop
4. Hardisk 500GB

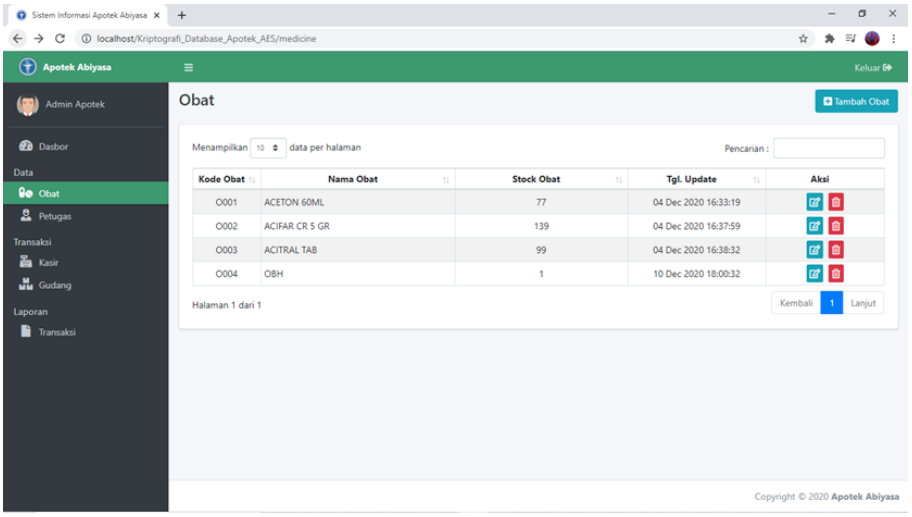
Perangkat Lunak

1. Sistem Operasi Windows 10
2. MySQL
3. PHP 7.3.12
4. Xampp V3.2.4
5. Firefox

F. Tampilan Layar

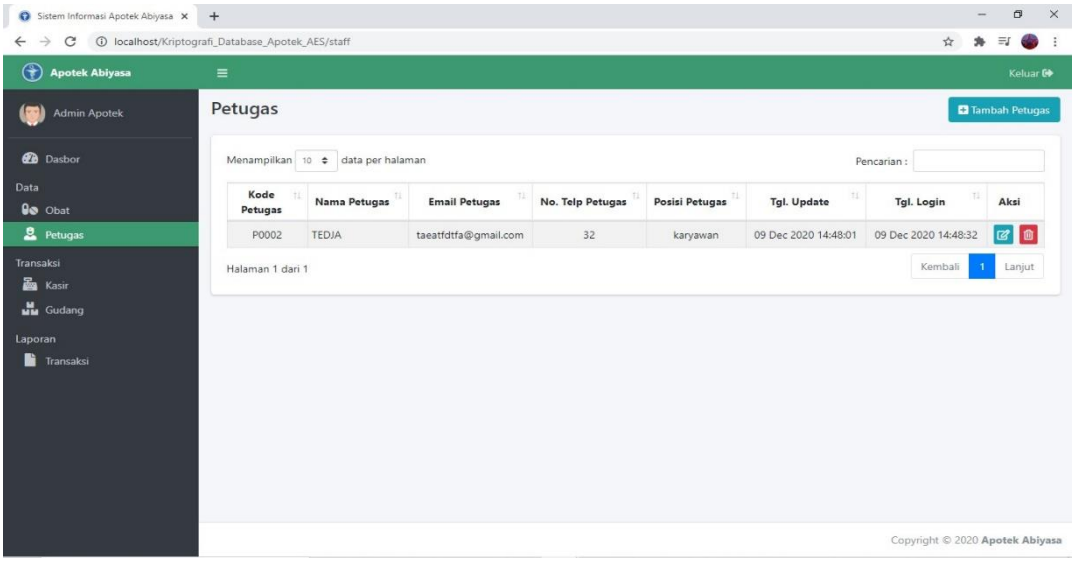
Pada bagian ini, menjelaskan mengenai tampilan layar aplikasi Pengamanan Basis Data Obat-obatan dengan Algoritma *Advanced Encryption Standard* 128. Berikut ini akan diberikan penjelasan dari beberapa tampilan yang ada. Pada tampilan layar halaman obat terdapat informasi tentang tabel yang menampilkan kode obat, nama obat, stok obat, tanggal *update* dan aksi. Di halaman ini terdapat *field* pencarian obat. Pada halaman ini juga terdapattombol tambah obat untuk menambahkan obat baru, dan terdapat tombol*edit* untuk mengubah data dari obat dan tombol hapus untuk menghapus obat dari tabel. Serta tombol keluar untuk kembali ke halaman *login*. Gambar 15 adalah tampilan layar halaman obat.

p-ISSN : 2443-2210
e-ISSN : 2443-2229



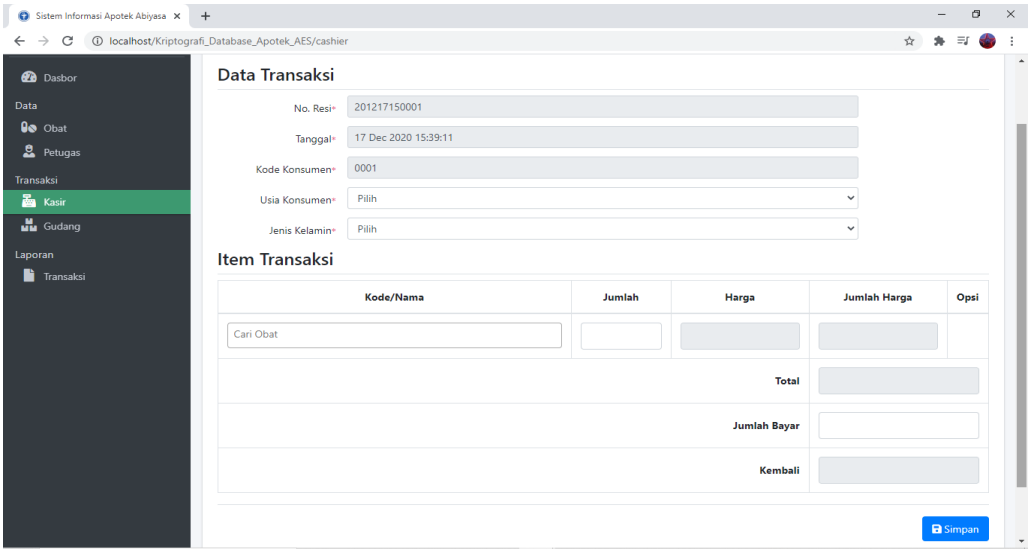
Gambar 15. Tampilan Layar Halaman Obat

Pada halaman ini, terdapat tabel yang berisikan kode petugas, nama petugas, email petugas, No. telepon petugas, tanggal *update*, tanggal *login* dan aksi.Dalam halaman ini juga terdapat tombol edit untuk mengubah informasi dari petugas dan tombol hapus untuk menghapus data petugas yang ada dari tabel. Pada halaman ini juga dilengkapi dengan tombol tambah petugas untuk menambahkan petugas baru ke dalam tabel dan tombol keluar untuk kembali ke halaman *login.* Gambar 16 adalah tampilan layar halaman petugas.



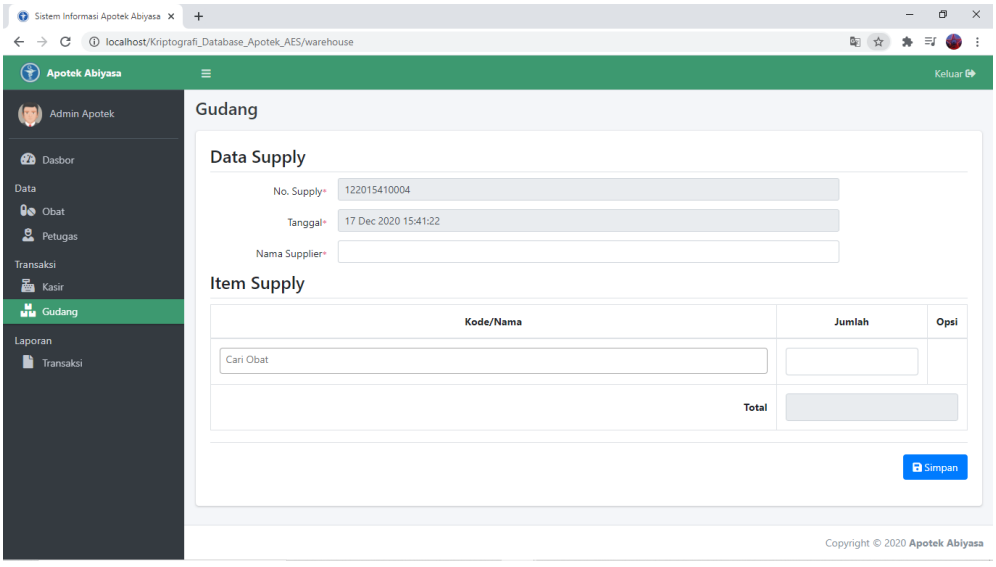
Gambar 16. Tampilan Layar Halaman Petugas

Pada halaman ini, berupa data transaksi dengan *field* No. resi, tanggal, kode konsumen, total dan kembali yang terisi secara otomatis. Pada halaman ini juga terdapat *field* usia konsumen, jenis kelamin dan jumlah bayar yang harus diisi kasir. Halaman ini juga terdapat tabel informasi obat yang dibeli yang berisikaninformasi tentang nama obat, jumlah, harga, jumlah harga, total, jumlah bayar dan uang kembali jika ada serta pada halaman ini juga dilengkapi dengan tombol hapus untuk menghapus obat dari *list* transaksi, serta tombol simpan untuk menyimpan transaksi yang sudah disetujui. Gambar 17 adalah tampilan layar halaman kasir.



Gambar 17. Tampilan Layar Halaman Kasir

Halaman ini, terdapat data berupa *field* No. *supply*, tanggal dan total yang terisiotomatis dan *field* nama *supplier* yang harus diisi *user*. Pada halaman inijuga terdapat tabel yang berisi informasi item seperti nama/kode, jumlah dan opsi hapus untuk menghapus obat yang ada di tabel. Pada halaman ini dilengkapi dengan tombol simpan untuk menyimpan informasi obat yang ditambahkan oleh *user* ke halaman obat. Gambar 18 adalah tampilan layar halaman gudang.



Gambar 18. Tampilan Layar Halaman Gudang

G. *Testing*

Tahap pengujian yang dilaksanakan ialah penggunaan Algoritma *Advanced Encryption Standard* (AES) pada tiap-tiap form yang ada dalam aplikasi dibuat. *Testing* ini dilaksanakan untuk mengetahui data yang dimasukkan telah terenkrip atau belum di *database*.

Hasil enkripsi dari aplikasi Pengamanan Basis Data Obat-obatan dengan Algoritma *Kriptografi Advanced Encryption Standard* (AES128) pada *database*, meliputi halaman obat, halaman petugas, halaman kasir dan halaman gudang. Tampilan gambar 19 ialah hasil enkripsi dari tabel *database* obat-obatan, yang berisikode_obat, nama_obat, satuan_obat, harga_obat, stok_obat dan tgl_update dimana nama_obat, satuan_obat, harga_obat, stok_obat dan tgl_update menjadi pesan acak.

kode_obat	nama_obat	satuan_obat	harga_obat	stok_obat	tgl_update
O001	FgNu6V8Cyl/s0jucyen7QenrIQ==	FgPefl8Cyl+4gtHZoA==	FgNon18Cyl8obD/c	igKFotsB0l/zgA==	FwPrxl8Cyl+uY3DhCKkAFxu2mU1Oyv2w115h
O002	0gCOSHcDyl+BJOnDp1TLRlgSmNxNSg==	0wAyGHcDyl/okfgJ	0wAXFHcDyl9vBjcP	cgERO5Pn0l/s+R0=	0wAlV3cDyl/n37tSbtjNUvT8C5zUxTcL2A7E
O003	QwAhIJgDyl8ZlHIz4arCbjpWog==	RABXQ5gDyl86MuJs+w==	RAC/4ZgDyl9zbToz	4QMgn04B0l/bOw==	RAAa/5gDyl8XOw+G/PQggBr6b5LBb62UByGX
O004	kQLUOdD/0V9Egtl=	kglpvtD/0V8XYx0=	kwLiEdD/0V+dBsbLfQ==	HQLtVdsB0l/2	IALIbtD/0V+qODqrgjD/m7c15Sc9JAa0woL2

Gambar 19. Hasil enkripsi data obat

Tampilan gambar 20 ialah hasil enkripsi dari tabel *database* petugas, yang berisi kode_petugas, nama_petugas, jenkel_petugas, notelp_petugas, email_petugas, alamat_petugas, posisi_petugas dan tgl_update dimana nama_petugas, jenkel_petugas, notelp_petugas, email_petugas, alamat_petugas, posisi_petugas dan tgl_update telah di enkripsi menjadi pesan acak.

kode_petugas	nama_petugas	jenkel_petugas	notelp_petugas	email_petugas	alamat_petugas	posisi_petugas
P0001	3gKzTCu7yl+No4p7jAvexN2lHiQ=	UgFVZpThyV/u	3gL4piu7yl/JHCpQOEXDbiSm0Q==	3wl23Cu7yl+a1OXeLgLFf+Bug4lNBY7YBK9E9G2Lww==	UwEYhZThyV/AqlS0CdB9mKr7xx5Vjw==	UwHunJThyV9D
P0002	zQHC4jGB0F8989zfyg==	zgHnPTGB0F9o	zgH6KzGB0F9Gag==	zwE2ZDGB0F/mSYrbRCKzXkpDA7TK76xliAWsqg==	0AFq2TGB0F90VK2flCY=	0AGyAzGB0F/a

Gambar 20. Hasil Enkripsi data petugas

Tampilan gambar 21 ialah hasil enkripsi dari *database* tabel kasir, yang berisi no_resi, kode_obat dan jumlah di mana hanya data jumlah saja yang di enkripsi menjadi pesan acak.

no_resi	kode_obat	jumlah
201211100001	O002	OgF7qJPn0l9J

Gambar 21. Hasil Enkripsi data transaksi pada kasir

Tampilan gambar 22 ialah hasil enkripsi dari *database* tabel gudang, yang berisi no_resi, kode_obat dan jumlah dimana hanya data jumlah yang di enkripsi menjadi pesan acak.

no_supply	kode_obat	jumlah
122014250003	O004	aQCsVwt80F8K
122014380003	O005	2wE5QPl+0F+5Icg=
122017440001	O001	SACuyh0Tyl/DqFo=
122017440001	O002	TAA9wB0Tyl9Gbo0=
122017440001	O003	UQBm6x0Tyl9Ag7Q=
122017450002	O002	uQCv70UTyl9MYA==
122018080003	O004	wACcca4B0l+6

Gambar 22. Hasil Enkripsi data Gudang

H. Algoritma Tahap Enkripsi dan Deskripsi AES-128

Algoritma 1 ialah algoritma tahap enkripsi AES dijelaskan seperti di bawah.

1) Start
2) Plain text
3) Add RoundKey
4) Substitution Byte
5) Shifft Row
6) Mix Columns
7) Add RoundKey
8) If round < 9 then
9) Mengulang ke baris 4
10) Else
11) Subsitution Byte
12) Shift Row
13) Add RoundKey
14) Cipher text
15) End
16) End if

Algoritma 1. Algoritma Enkripsi

Algoritma 2 adalah algoritma dari tahap dekripsi AES dapat dilihat seperti dibawah ini.

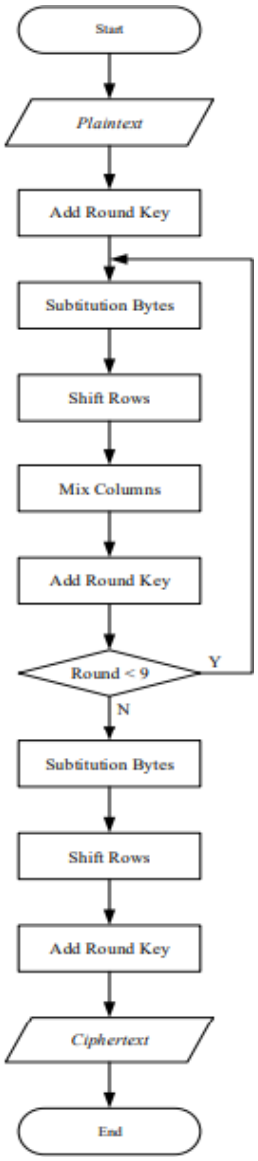
1) Start
2) Cipher text
3) Add RoundKey
4) Inv Shift Row
5) Inv Substitution Byte
6) Add RoundKey
7) Inv MixColumns
8) If round < 9 then
9) Mengulang ke baris 4
10) Else
11) Inv Shift Row
12) Inv SubstitutionKey
13) Add RoundKey
14) Plain text
15) End if

Algoritma 2. Algoritma Deskripsi

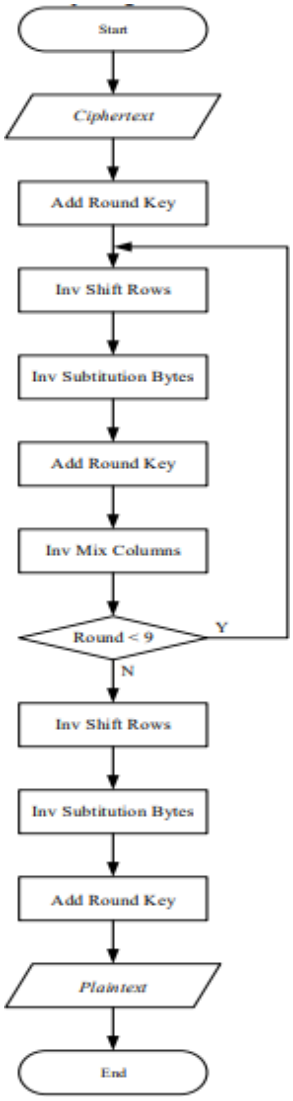
I. Flowchart Tahap Enkripsi AES-128

Flowchart ini menampilkan tahap enkripsi dan dekripsi dari *plaintext* ke *ciphertext* dan sebaliknya dari *ciphertext* ke *plaintext* dimana proses enkripsi dari *plaintext* ke *chipertext* pada AES-128 diperlihatkan pada gambar 23, dan proses selanjutnya yaitu dekripsi proses perubahan dari *ciphertext* ke *plaintext* pada AES-128 diperlihatkan pada gambar 24.

p-ISSN : 2443-2210
e-ISSN : 2443-2229



Gambar 23. *Flowchart* Proses Enkripsi AES-128



Gambar 24. *Flowchart* Proses Dekripsi AES-128

Pengujian ini dilakukan agar mengetahui panjang dari simbol yang dihasilkan tahap enkripsi-dekripsi dengan metode *Advanced Encryption Standard* 128 dan perbandingannya dengan panjang teksaslinya apa ukuran panjang sama dengan jumlah *character* yang dikirimkan. Dinyatakan linier pada ukuran panjang hasil enkripsi berbeda dari panjang *character text* aslinya. Tabel 1 dan 2 merupakan hasil enkripsi-deskripsi *Advanced Encryption Standard* (AES-128).

TABEL 1
TABEL PENGUJIAN 1 HASIL ENKRIPSI-DEKRIPSI AES-128

Data	KarakterAsli	Jumlah Karakter(bit)	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi (bit)
nama_obat	ACETON 60ML	11	FgNu6V8Cyl/s0jucyen7QenrlQ==	28
satuan_obat	Botol	5	FgNu6V8Cyl/s0jucyen7QenrlQ==	28
harga_obat	6.750	5	FgNon18Cyl8obD/c	16
stok_obat	77	2	igKFotsB0l/zgA==	16
tgl_update	04 Dec 2020 16:33:19	20	FwPrxl8Cyl+uY3DhCKkAFxu2mU1Oyv2w115h	36

TABEL 2
TABEL PENGUJIAN 2 HASIL ENKRIPSI-DEKRIPSI AES-128

Data	KarakterAsli	Jumlah Karakter(bit)	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi (bit)
nama_obat	ACITRALTAB	11	QwAhIJgDyl8ZlHIz4arCbjpWog==	28
satuan_obat	Strip	5	RABXQ5gDyl86MuJs+w==	20
harga_obat	1.380	5	RAC/4ZgDyl9zbToz	16
stok_obat	99	2	4QMgn04B0l/bOw==	16
tgl_update	04 Dec 2020 16:38:32	20	RAAa/5gDyl8XOw+G/PQggBr6b5LBb62UbyGX	36

Kelebihan dari sistem ini adalah isi data akan aman saat diinput karena data yang di input sudah terenkripsi, aplikasi yang mudah digunakan serta informasi transaksi yang cukup lengkap. Namun tetap saja masih ada kekurangan dari segi tampilan yang masih sederhana serta akun administrator belum bisa lebih dari 1 akun.

IV. SIMPULAN

Berdasarkan hasil serta analisis yang telah dilaksanakan dengan masalah-masalah pada aplikasiyang dibuat, maka bisa ditarik kesimpulan untuk pengembangan aplikasi ke tahap yang lebih baik. Pada pembahasan diatas, maka dapat disimpulkan bahwa implementasi Algoritma kriptografi *Advanced Encryption Standard* 128 (AES-128) telah berhasil dan digunakan sesuai kebutuhan Apotek, dengan aplikasi ini pihak Apotek dapat menyimpan data obat-obatan di *database* dengan aman. Karena dengan proses enkripsi, data-data yang disimpan dalam *database* Apotek tersimpan dengan data berupa kode acak, sekaligus mengamankan informasi data pada Apotek dari pihak yang tidak bertanggung jawab.

DAFTAR PUSTAKA

[1] Murdowo and Sugeng, "Mengenal Proses Perhitungan Enkripsi Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) Rijdnael," *INFOKAM,* vol. 10, no. 1, p. 32–40, 2014.

[2] Rahmawati, Rika and D. Rahardjo, "Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi AES-128 BIT Pada SMK PGRI 15 Jakarta," *Jurnal Teknik Informatika dan Sistem Informasi,* vol. 2, no. 1, p. 67–74, 2016.

[3] Gunadhi, Erwin and H. Abdurachman, "Keamanan Komunikasi Data SMS Pada Android dengan Menggunakan Aplikasi Kriptografi Advanced Encryption Standard (AES)," *Jurnal Sekolah Tinggi Teknologi Garut,* vol. 12, no. 2, p. 296–300, 2015.

[4] Tullah, Rahmat, Y. Permanasari and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA,* vol. 15, no. 1, p. 7–14, 2016.

[5] A. D. Ananto, R. M and B. Irawan, "Desain dan Implementasi Aplikasi SMS (Short Message Service) Pada Android Menggunakan Algoritma AES-128," *Jurnal eProceeding of Engineering,* vol. 2, no. 2, p. 3318–3326, 2015.

[6] I. Suryanto, C. Suhery and Y. Brianorman, "Pengembangan Aplikasi Chat Messenger Dengan Metode Advanced Encryption Standard (AES) Pada Smartphone," *Jurnal Coding Sistem Komputer Untan,* vol. 5, no. 2, pp. 1-12, 2017.

[7] Permana, A. Aditya and D. Nurnaningsih, "Rancangan Aplikasi Pengaman Data Dengan Algoritma Advanced Encryption Standard (AES)," *Jurnal Teknik Informatika,* vol. 11, no. 2, p. 177–186, 2018.

[8] V. Novianty and R. E. Gunadhi, "Mengamankan Basis Data Keuangan Koperasi dengan Menggunakan Kriptografi Advanced Encryption Standard (AES)," *Jurnal Algoritma Sekolah Tinggi Teknologi Garut,* vol. 12, no. 2, p. 179–185, 2015.

[9] F. A. Sianturi, "Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advances Encryption Standard (AES)," *Pelita Informatika Budi Darma,* vol. 4, no. 1, p. 42–46, 2013.

[10] Rahmayunita, Isnawaty and Sutardi., "Penyadapan SMS dan GPS Berbasis Android Menggunakan Algoritma Advanced Encryption Standard (AES)," *SemanTIK,* vol. 1, no. 2, p. 11–22, 2015.

[11] R. Primartha, "Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Advens Encryption Standard (AES)," *Journal of Research in Computer Science and Applications,* vol. 2, no. 1, pp. 1-19, 2013.

[12] A. Rosyadi, "Implementasi Algoritma Kriptografi Aes Untuk Enkripsi Dan Dekripsi Email," *Jurnal Ilmiah Teknik Elektro,* vol. 1, no. 3, p. 63–67, 2012.