Journal Global Tecnology Computer
Vol 1, No. 3, Agustus, 2022, Hal 77 - 83
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Penerapan Algoritma Aes 625 Dalam Pengamanan Data Rekam Medis

Putri Yosi Tanjung H

Teknik Informatika, Ilmu Komputer Dan Teknologi Informasi, Universitas Budi Darma, Indonesia
Jl. Sisingamangaraja No. 338, Medan, Sumatera Utara, Indonesia
Email: putriyoshitanjung12@gmail.com

Abstrak−Rekam medis adalah data yang bersifat sangat pribadi dan menjadi salah satu informasi penting Yang harus dimiliki oleh seorang pasien. Rekam medis berisi tentang catatan-catatan kesehatan pasien seperti identitas pasien, riwayat penyakit pasien, diagnose,dan tindakan dokter. Rekam medis dianggap sebagai data rahasia yang hanya boleh dibuka oleh pihak-pihak tertentu. Salah satu cara untuk menyimpan dan menjaga kerahasiaan data rekammedis adalah dengan menggunakan metode AES 256. Metode yang dirujuk untuk melakukan pengamanan data adalah dengan menggunakan sebuah Algoritma kriptografi, yaitu sebuah algoritma yang digunakan untuk melakukan enkripsi dan dekripsi. Dengan penerapan algoritma ini data sensitive pada rekam medis dapat dijaga kerahasiannya dan tidak mempengaruhi terhadap kecepatan akses aplikasi.

Kata Kunci: Pengamanan Data, Rekam Medis, Kriptografi, Enkripsi, Dekripsi, AES 256.

Abstract− Medical records are data that are very personal and become one of the important information that must be owned by a patient. The medical record contains the patient's health records such as the patient's identity, patient history, diagnosis, and doctor's actions. Medical records are considered as confidential data that may only be disclosed by certain parties. One way to store and maintain the confidentiality of medical record data is to use the AES 256 method. The method referred to for data security is to use a cryptographic algorithm, which is an algorithm used to perform encryption and decryption. With the application of this algorithm, sensitive data in medical records can be kept confidential and does not affect the speed of application access.

Keywords: Data Security, Medical Records, Cryptography, Encryption, Decryption, AES 256.

1. PENDAHULUAN

Seiring dengan memasuki era *internet* dimana perkembangan pertukaran informasi pun berkembang pesat. Kini informasi berupa pesan dan gambar dapat dikirimkan sebagai surat elektronik melalui *e-mail*, dipajang di *blog* pribadi sebagai *post* berita, maupun yang belakangan ini populer adalah memajangnya di *social networking* seperti *facebook*, *friendster*, dan *twitter*. Dengan adanya layanan untuk bertukar informasi di internet dengan memanfaatkan media *online* ini, maka dibukalah lembaran baru dalam metode bertukar informasi.

Rekam medik adalah berkas yang berisi catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien. Informasi yang baik dan berguna dapat sangat penting dalam menolong seseorang dalam kondisi tertentu, informasi yang komprehensif sebelum melakukan intervensi klinis. Sistem pelayanan rekam medis bertujuan menyediakan informasi guna memudahkan pengelolaan dalam pelayanan kepada pasien dan memudahkan pengambilan keputusan. Pada prinsipnya isi Rekam Medis adalah milik pasien, sedangkan berkas Rekam Medis (secara fisik) adalah milik Rumah Sakit atau institusi kesehatan. Berkas rekam medis itu merupakan milik sarana layanan kesehatan, yang harus disimpan sekurang-kurangnya untuk jangka waktu 5 tahun terhitung sejak tanggal terakhir pasien berobat [1].

Data yang ada pada rekam medis ini bersifat rahasia sehingga perlu untuk dilakukan pengamanan terhadap data-data tersebut. Keamanan data rekam medis adalah hal yang sangat penting, apalagi data rekam medis adalah data yang sangat rahasia. Berbagai usaha dilakukan untuk menjamin agar data rahasia tersebut tidak bisa diakses oleh pihak lain.

Hal tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak. Jika hal tersebut sampai terjadi, kemungkinan besar akan merugikan pihak pasien. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh pasien maupun dokter. Selain itu data yang dibajak tersebut akan memiliki kemungkinan rusak bahkan hilang. Maka dari itu upaya yang dilakukan untuk melakukan pengamanan data tersebut yaitu dengan melakukan enkripsi. Metode yang digunakan dalam penelitian ini menggunakan Kriptografi AES 256.

Algoritma AES merupakan algoritma chiper yang aman untuk melindungi data atau informasi yang bersifat rahasia. AES dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001 yang digunakan untuk menggantikan algoritma DES yang sudah dianggap kuno dan mudah dibobol. Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi chipertext. Panjang kunci dari AES terdiri dari panjang kunci 128 bit, 192 bit, dan 256 bit. Perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES ini. Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi chipertext. Panjang kunci dari AES terdiri dari panjang kunci 128 bit, 192 bit, dan 256 bit. Perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES ini. Jumlah putaran yang digunakan algoritma ini ada tiga macam seperti pada tabel di bawah [2].

2. METODOLOGI PENELITIAN

2.1 Kerangka Kerja Penelitian

Dalam penelitian ini penulis melakukan beberapa penerapan metode penelitian untuk menyelesaikan permasalahan. Adapun metode penelitian yang dilakukan adalah dengan cara:

a. Studi Literatur
   Pada tahap ini dilakukan proses pengumpulan informasi yang diperlukan untuk proses perancangan system yaitu mempelajari buku, artikel, atau situs yang memuat atau mempelajari perangkat lunak Visual Basic.Net untuk mengetahui fungsi dan aplikasi.
b. Analisa
   Melakukan analisa masalah proses enkripsi dan dekripsi dalam melakukan pengamanan data rekam medis, mempelajari perangkat lunak Visual Basic.Net secara umum, analisis kebutuhan umum sistem, analisis kerja dan analisis kebutuhan perangkat lunak serta modul.
c. Perancangan
   Melanjutkan analisa perangkat lunak yang sudah dilaksanakan sebelumnya ke tahapan selanjutnya, yaitu perancangan arsitektur perangkat lunak, kerja, modul, basis data dan perancangan antar muka serta lingkungan pengembangan perangkat lunak
d. Implementasi
   Melakukan implementasi dari hasil perancangan yang sudah dilakukaan sebelumnya kedalam suatu aplikasi pengamanan data
e. Pengujian Perangkat Lunak
   Pengujian perangkat lunak yang sudah dikembangkan dengan sistematika yang sudah dirancang sedemikian rupa untuk melihat perangkat lunak memberikan hasil yang diinginkan.
f. Penulis Laporan Penelitian
   Pada tahap ini penulis menuangkan seluruh hasil riset dalam bentuk buku..

2.2 Kriptografi

Kriptografi (Cryptography) merupakan cabang ilmu pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi data. Teknik ini digunakan untuk mengkonversi atau mengubah data ke dalam bentuk kode-kode tertentu, dengan tujuan informasi yang disimpan maupun ditransmisikan melalui jaringan yang tidak aman seperti internet, tidak dapat dibaca oleh siapapun kecuali oleh orang yang berwenang. Kriptografi adalah suatu ilmu yang menciptakan suatu komunikasi secara aman yang tidak dapat dimengerti atau diterjemahkan oleh setiap orang kecuali orang tertentu yang dimaksud [3].

2.3 Rekam Medis

Rekam medis adalah berkas yang berisi catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien. Tujuan terselenggaranya pelayanan rekam medis adalah untuk menunjang tercapainya tertib administrasi. Tanpa adanya suatu sistem pengelolaan rekam medis yang baik dan benar, mustahil tertib administrasi rumah sakit berhasil sebagaimana yang diharapkan [8] [9].

2.4 Algoritma AES 256

Algoritma AES merupakan algoritma chiper yang aman untuk melindungi data atau informasi yang bersifat rahasia. AES dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001 yang digunakan untuk menggantikan algoritma DES yang sudah dianggap kuno dan mudah dibobol. Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi chipertext. Panjang kunci dari AES terdiri dari panjang kunci 128 bit, 192 bit, dan 256 bit. Perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES ini. Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi chipertext [2].

3. HASIL DAN PEMBAHASAN

Rekam medis elektronik telah menjadi keharusan dalam pencatatan sejarah kondisi kesehatan bagi setiap pasien. Pencatatan ini melibatkan instansi pelayanan kesehatan, para petugas kesehatan, apoteker, dan pasien. Masalah yang sering muncul adalah keamanan dari rekaman itu sendiri dari berbagai pihak yang dapat menyalahgunakan. Ini akan sangat berdampak pada semua yang terlibat utamanya pada pasien. Pasien akan mendapatkan kerugian besar baik materil maupun psikologis. Beberapa solusi telah diusulkan seperti pencatatan terpusat, penerapan enkripsi, verifikasi berulang.

Journal Global Tecnology Computer
Vol 1, No. 3, Agustus, 2022, Hal 77 - 83
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Tabel 1. Data Rekam Medis

No	No Kartu	Tgl Pemeriksaan	Nama	Tgl Lahir	Jenis Kelamin	Alamat	Tinggi Badan	Berat Badan	Keluhan	Tekanan Darah	Respiratory Rate	Nama Penyakit	Nama Obat
1	0100001	29/07/2016	Agung Sutrajad	18/06/1993	Laki-laki	Jl. Sakti Lubis	169	59	Sakit Kepala	120/80	120	Hipertensi Primer (essensial)	Propanolol HCI Table 40 Mg
2	0100002	31/07/2016	Nani	18/06/1986	Wanita	Jl. Garu I	155	50	Sakit Maag	100/70	100	Tukak Lambung	Antasida DOEN I table Kunyah

3.1 Implementasi Algoritma

3.1.1 Proses Enkripsi

Untuk proses enkripsi AES 256, plaintext di transformasikan secara berulang kali selama beberapa putaran. Banyaknya transformasi putaran (Nr) tergantung dari nilai Nk dan Nb. Nk yaitu panjang kunci dibagi 32, sedangkan Nb yaitu panjang blok dibagi 32.

Plaintext: 010000120160729

Kunci : YOSI dikonversikan ke dalam bilangan *biner* maka menjadi 01111001 01101111 01110011 01101001

a. Mengekspansi Kunci:

W1 = 01111001 W2 = 01101111

W3 = 01110011 W4 = 01101001

Rcon yang digunakan adalah: 01 02 04 08 10 20 40 80 1b 36. Proses pencariannya adalah sebagai berikut

Cipher Key Kolom IV		Penggeseran Posisi Baris		Hasil
01		10		d7
10	RotWord	10	SubByte	ab
10		01		76
01		01		fe

maka:

Cipher Key KolomIV I		Hasil		Rcon		Round Key kolom
01		d7		01		d6
11	⊕	ab	⊕	11	=	aa
10		76		10		74
01		fe		01		fd

Untuk mendapatkan Round Key kolom II sampai kolom IV tidak perlu di XOR kan dengan Rcon, Rcon hanya digunakan untuk mendapatkan byte kolom I tiap putaran.

Maka:

Cipher Key Kolom II		Round Key kolom I		Round Key kolom II
01		d6		d2
10	⊕	aa	=	af
11		74		72
11		fd		fa

Tabel 2. Round Constanta (Rcon)

01	02	04	08	10	20	40	80	1b	36
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

Tabel 3. Round Key Enkripsi

Cipher Key				Round Key I				Round Key II				Round Key III			
01	01	01	01	d6	d2	da	d6	b6	64	be	68	B6	d2	6c	04
11	10	11	10	aa	Af	a6	ab	92	3d	9b	30	Ff	c2	59	69
10	11	00	10	74	72	78	76	Cf	bd	c5	b3	74	c9	0c	Bf
01	11	11	01	fd	Fa	f1	fa	0b	f1	00	fe	4e	bf	bf	41

Tabel 4. Round Key Enkripsi

Round Key IV				Round Key V				Round Key VI				Round Key VII			
47	95	f9	fd	3c	a9	50	ad	5e	f7	a7	0a	14	E3	44	4e
f7	35	6c	05	Aa	9f	f3	f6	39	a6	55	a3	f9	5f	0a	a9

f7	3e	32	8d	a3	9d	af	22	0f	92	3d	1f	70	e2	df	C0
bc	03	bc	fd	e8	Eb	57	aa	7d	96	c1	6b	1a	8c	4d	26

Tabel 5. Round Key Enkripsi

Round Key VIII				*Round Key* IX				*Round Key* X			
47	a4	e0	ae	54	f0	10	be	13	e3	f3	4d
43	1c	16	bf	99	85	93	2c	11	94	07	2b
87	65	ba	7a	32	57	ed	97	1d	4a	A7	30
35	b9	f4	d2	d1	68	9c	4e	7f	17	8b	c5

b. Melakukan penjumlahan bit antara blok plaintext dengan kunci.
Plaintext cipher key Key Addition

00 44 88 cc ⊕ 00 04 08 0c = 00 40 80 c0
11 55 99 dd ⊕ 01 05 09 0d = 10 50 90 d0
22 66 Aa ee ⊕ 02 06 0a 0e = 20 60 a0 e0
33 77 bb ff ⊕ 03 07 0b 0f = 30 70 b0 f0

c. Melakukan transformasi putaran sebanyak Nr kali sebagai berikut: Nk =128/32 =4
Nb =128/32 =4
Maka Nr=10 putaran.
Putaran:

1. Sub Byte

00 40 80 c0		63 09 cd ba
10 50 90 d0	S-Box	ca 53 60 70
20 60 a0 e0		b7 d0 e0 e1
30 70 b0 f0		04 51 e7 8c

2. Shift Row

63 09 cd ba		63 09 cd ba
ca 53 60 70	Shift Row	53 60 70 ca
b7 d0 e0 e1		e0 e1 b7 d0
04 51 e7 8c		8c 04 51 e7

3. Mix Column
Pada proses ini hasil dari Shift Row di-XOR-kan dengan matriks yang telah ditentukan:
=(63)(02) ⊕ (53)(03) ⊕ (e0)(01) ⊕ (8c)(01)
=(01100011)(00000010) ⊕(01010011)(00000011)
(11100000)(00000001)⊕(10001100)(00000001)
= (x6+x5+x+1)(x)⊕(x6+x4+x+1)(x+1)⊕(x7+x6+x5)(1)⊕(x7+x3+x2)(1)
=(x6+x4+x3+x2+x+1)
=01011111
=5f
Proses ini dilakukan tiap putaran yaitu dari putaran pertama hingga putaran kesembilan. Pada putaran kesepuluh, proses inidiabaikan.

$$\begin{bmatrix}02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02\end{bmatrix}\begin{bmatrix}63 & 09 & cd & ba\\ 53 & 65 & 70 & ca\\ e0 & e1 & b7 & d0\\ 8c & 04 & 51 & e7\end{bmatrix}=\begin{bmatrix}5f & 57 & f7 & 1d\\ 72 & f5 & be & b9\\ 64 & bc & 3b & f9\\ 15 & 92 & 29 & 1a\end{bmatrix}$$

4. Add Round Key
Hasil MixColum Round Key I Hasil

$$\begin{bmatrix}5f & 57 & f7 & 1d\\ 72 & f5 & be & b9\\ 64 & bc & 3b & f9\\ 15 & 92 & 29 & 1a\end{bmatrix}\begin{bmatrix}d6 & d2 & da & d6\\ aa & af & a6 & ab\\ 74 & 72 & 78 & 76\\ fd & fa & f1 & fa\end{bmatrix}=\begin{bmatrix}89 & 85 & 2d & cb\\ d8 & 5a & 18 & 12\\ 10 & ce & 43 & 8f\\ e8 & 68 & d8 & ed\end{bmatrix}$$

Untuk putaran dari dilakukan sebanyak 10 putaran Dari beberapa langkah di atas diperoleh ciphertext sebagai berikut:
69c4e0d86a7b0430d 8cdb78070b4c55a

3.1.2 Proses Dekripsi

Pada proses dekripsi AES 256 hal-hal kunci dan ciphertext harus diketahui.
Ciphertext : 69c4e0d86a7b0430d8cdb78070b4c55a
kunci : 01111001 01101111 01110011 01101001

Journal Global Tecnology Computer
Vol 1, No. 3, Agustus, 2022, Hal 77 - 83
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

Maka proses pendekripsian nya adalah sebagai berikut:

a. Mengkspansi Kunci
Kunci yang telah diekspansi:
W1 = 01111001 W2 = 01101111
W3 = 01110011 W4 = 01101001
Proses pencariannya sebagai berikut:

Cipher Key Kolom IV		**Penggeseran Posisi Baris**		**Hasil**
0c		0d		d7
10	Rot Word	10	Sub Byte	ab
10		01		76
01		01		fe

Cipher Key Kolom IV	**Hasil**	**Rcon**		**Round Key kolom**
01	D7	01		D6
11	Ab	00	=	aa
10	76	00		74
01	Fe	00		fd

Untuk mendapatkan Round Key kolom II sampai kolom IV tidak perlu di XOR kan dengan Rcon, Rcon hanya digunakan untuk mendapatkan byte kolom I tiap putaran.
Maka:

Cipher Key Kolom II	**Round Key kolom I**		**Round Key kolom II**
01	d6		d2
10	Aa	=	af
11	74		72
11	Fd		fa

Tabel 6. Round Key Dekripsi

Cipher Key				**Round Key I**				**Round Key II**				**Round Key III**			
01	01	01	01	d6	d2	da	d6	b6	64	be	68	B6	d2	6c	04
11	10	11	10	aa	Af	a6	ab	92	3d	9b	30	Ff	c2	59	69
10	11	00	10	74	72	78	76	cf	bd	c5	b3	74	c9	0c	bf
01	11	11	01	fd	Fa	f1	fa	0b	f1	00	fe	4e	bf	bf	41

Tabel 7. Round Key Dekripsi

Round Key IV				**Round Key V**				**Round Key VI**				**Round Key VII**			
47	95	f9	fd	3c	a9	50	ad	5e	f7	a7	0a	14	E3	44	4e
f7	35	6c	05	aa	9f	f3	f6	39	a6	55	a3	f9	5f	0a	a9
f7	3e	32	8d	a3	9d	af	22	0f	92	3d	1f	70	e2	df	C0
bc	03	bc	fd	e8	Eb	57	aa	7d	96	c1	6b	1a	8c	4d	26

Tabel 8. Round Key Dekripsi

Round Key VIII				**Round Key IX**				**Round Key X**			
47	a4	e0	ae	54	f0	10	be	13	e3	f3	4d
43	1c	16	bf	99	85	93	2c	11	94	07	2b
87	65	ba	7a	32	57	ed	97	1d	4a	A7	30
35	b9	f4	d2	d1	68	9c	4e	7f	17	8b	c5

b. Putaran
1. Inverse of Add Round Key

Journal Global Tecnology Computer
Vol 1, No. 3, Agustus, 2022, Hal 77 - 83
ISSN: **2809-6118** (Online - Elektronik)
Website https://ejurnal.seminar-id.com/index.php/jogtc

69	6ad8	70		13	e3	f3	4d		7a89	2b	3d
c4	7b	cd	b4	⊕	11	94	07	2b	=	d5	efca9f
e0	04	b7	c5		1d	4a	a7	30		fd	4e10 f5
d8	30	80	5a		7f	17	8b	c5		a7	27 0b 9f

2. Inverse of Mix Column
   Pada putaran pertama proses ini tidak digunakan.
3. Inverse Shift Row

7a	89	2b	3d		7a89	2b	3d
d5	efca9f			InvShiftRow	9fd5	ef	ca
fd	4e10	f5			10	f5	fd 4e
a7	27	0b	9f		27	0b	9f a7

4. Inverse of Sub row

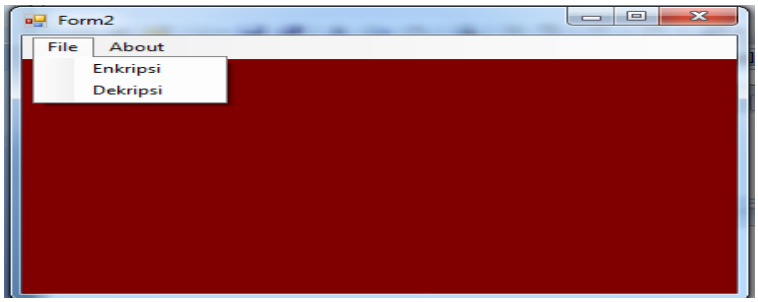
7a89	2b	3d			bd	f2	0b ab
9fd5	ef	ca		InvSubByte	6e	b5	a1 10
10	f5	fd	4e		7c	77	21 b6
27	0b	9f	a7		3d	9e	6e 89

Proses inverse terus dilakukan sampai dengan 10 putaran sehingga hasil dari proses dekripsi, plaintext nya adalah sebagai berikut: 010000120160729

3.2 Implementasi

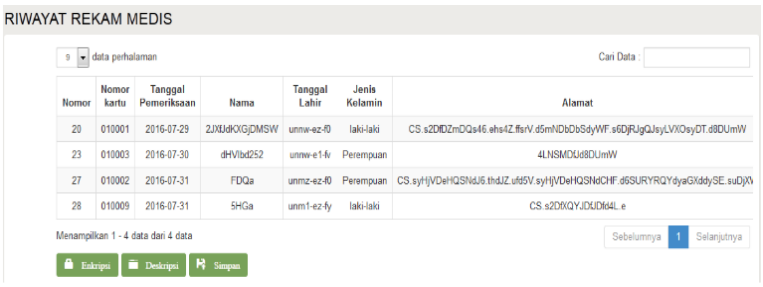
Implementasi adalah suatu tindakan atau pelaksanaan dari sebuah rencana yang sudah disusun secara matang dan terperinci. Implementasi biasanya dilakukan setelah perencanaaan sudah dianggap fix.

a. Tampilan Menu Utama
   Antarmuka menu utama adalah halaman yang muncul pertama kali saat sistem dijalankan. Antarmuka menu utama dapat dilihat pada gambar 1 berikut.



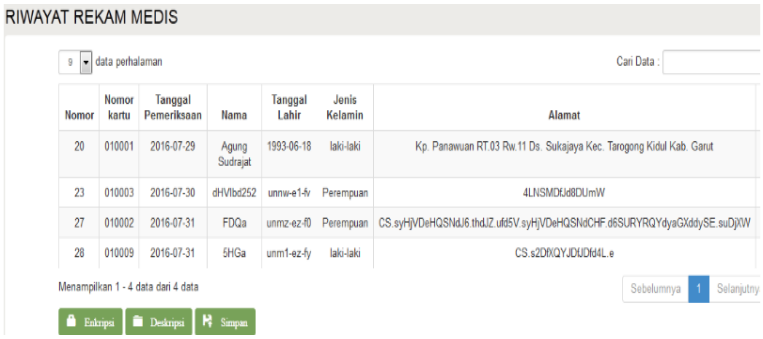
Gambar 1. Antarmuka Menu Utama

b. Tampilan Menu Enkripsi
   Penerapan enkripsi pada aplikasi rekam medis pasien, yaitu dengan melakukan enkripsi pada data-data yang dianggap penting dan rahasia yaitu dilakukan enkripsi pada data nama, tanggal lahir, alamat, keluhan, tekanan darah, respiatory rate, penyakit yang pernah diderita dan nama obat yang diberikan. Adapun tampilan dari menu enkripsi dapat di lihat pada gambar 2 di bawah ini.



Gambar 2. Tampilan Menu Enkripsi

c. Tampilan Proses Dekripsi
Untuk melakukan deskripsi yaitu dengan cara memilih data yang ingin dilakukan deskripsi kemudian tekan tombol deskripsi lalu selanjutnya tekan tombol simpan. Tampilan halaman menu dekripsi dapat dilihat pada gambar 3 berikut



Gambar 3. Tampilan Menu Dekripsi

4. KESIMPULAN

Kesimpulan yang didapat dari penulisan penelitian ini adalah Algoritma AES 256 ini dapat diterapkan untuk pengamanan aplikasi rekam medis pasien. Data yang ada pada rekam medis pasien menjadi lebih aman dari serangan para kriptanalis dengan menggunakan Algoritma AES 256. Dalam pengimplementasian pengamanan data rekam medis nmenggunakan visual basic.Net 2008

REFERENCES

[1] Nuraini, Novita, 2015, "*Analisis Sistem Penyelenggara Rekam Medis di InstalasiRekam Medis RS "X", Tangerang Periode April-Mei 2015",* Jurnal ARSI, Volume 1 Nomor 3.
[2] Bhaudayana. G.W, dkk. 2015. "*Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB Pada Gambar Bitmap",* Jurnal Ilmiah Ilmu Komputer Universitas Udayana, Vol 8, No.2.
[3] Sony Bahagia Sinaga, 2018, "*Pengamanan Pesan Komunikasi Menggunakan Algoritma Rsa, Rabbin Miller Dan Fungsi Sha-1 Serta Penanganan Man In The Middle Attack Dengan Interlock Protocol",* Jurnal Media Informasi Analisa dan Sistem (MEANS), Vol. 3, No.1.
[4] Ariyus, Dony, 2005, "*Kriptografi Keamanan Data Dan Komunikasi*". Edisi Pertama. Yogyakarta. Graha Ilmu.
[5] Sadikin, Rifki, 2012, *"Kriptografi Untuk Keamanan Jaringan",* Penerbit Andi, Yogyakarta.
[6] Ariyus, Dony, 2008, "*Computer Security,* Andi, Yogyakarta.
[7] https://aepnurulhidayat.wordpress.com/2016/06/09/pengertian-tujuan-kegunaan- dan- aspek-rekam-medis-presented-by-aep-nurul-hidayah/, diakses tanggal 27 Mei 2019.
[8] https://nisaahaniblog.wordpress.com/2016/07/15/teori-ascii-american-standard-code-for-information-interchange/, diakses tanggal 26 Mei 2019.
[9] Nuraini, Novita, 2015, "*Analisis Sistem Penyelenggaraan Rekam Medis Di Instalasi Rekam Medis RS "X" Tangerang Periode April-Mei 2015",* Jurnal ARSI, Volume 1, Nomor 3.
[10] A.S. Rosa dan Shalahuddin. M, 2013, "*Rekayasa Perangkat Lunak Terstruktur",* Andi, Yogyakarta.
[11] Aditya, Arif Primananda, 2013, *"Dasar-Dasar Pemrograman Database Dekstop Dengan Visual Basic. Net 2008,* PT. Elex Media Komputindo, Jakarta.