
IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA REKAM MEDIS DI KLINIK PRATAMA SITI RAHMAH MENGGUNAKAN METODE *ADVANCED ENCRYPTION STANDARD*

Nur Nia Suci ¹, Nurcahyo Budi Nugroho ², Sri Murniyanti ³

^{1,3} Program Studi Sistem Informasi, STMIK Triguna Dharma

² Program Studi Sistem Komputer, STMIK Triguna Dharma

Article Info

Article history:

Received, 201x

Revised, 201x

Accepted, 201x

Keyword:

Kriptografi

Data Rekam Medis

Advanced Encryption Standard

ABSTRACT

Rekam medis merupakan sebuah rekaman kesehatan yang memuat kumpulan data-data yang berisi tentang catatan riwayat kesehatan pasien seperti identitas pasien, hasil anamnesis, hasil pemeriksaan fisik dan catatan segala kegiatan para tenaga kesehatan terhadap pasien, data rekam medis merupakan salah satu data yang bersifat rahasia, data ini sangat rentan disalahgunakan atau di manipulasi oleh oknum yang tidak bertanggung jawab dan akan menimbulkan kerugian bagi instansi kesehatan.

*Dalam hal ini diperlukan sebuah sistem dalam pengamanan data yang dapat melakukan penyandian dan pengacakan sebuah informasi yang berbasis komputer. Pengamanan ini dilakukan dengan cara menerapkan sebuah algoritma kriptografi yang digunakan adalah algoritma *Advanced Encryption Standard*.*

Hasil Pengujian menunjukkan bahwa sistem keamanan data rekam medis dapat mengamankan data rekam medis dengan sangat baik dan menghindari terjadinya penyalahgunaan atau manipulasi data oleh oknum yang tidak bertanggung jawab.

Copyright © 2021 STMIK Triguna Dharma.

All rights reserved.

Corresponding Author:

Nama : Nur Nia Suci

Program Studi : Sistem Informasi

STMIK Triguna Dharma

Email : nurniasuci47@gmail.com

1. PENDAHULUAN

Perkembangan teknologi terutama pada sistem pengamanan data dalam menjaga keamanan data informasi telah berkembang pesat. Masalah keamanan data merupakan salah satu aspek penting dari sebuah Sistem Informasi. Seiring berkembangnya teknologi informasi semakin tinggi pula tingkat penyalahgunaan informasi tersebut. Keamanan data atau informasi adalah suatu hal yang harus diperhatikan. Dimana ada suatu data atau informasi yang sifatnya rahasia dan penting sehingga keberadaannya tidak boleh diketahui oleh pihak yang tidak berwenang, maka perlu menerapkan keamanan data yang baik.

Salah satu informasi atau data yang perlu dijaga keamanannya adalah data rekam medis dalam bidang kesehatan. Data rekam medis yaitu berkas catatan dan dokumen yang berisi identitas, pemeriksaan, pengobatan, tindakan medis lain pada sarana pelayanan kesehatan untuk rawat jalan, rawat inap baik dikelola pemerintah maupun swasta [1]. Contoh kasus penyalahgunaan data rekam medis di Rumah Sakit Samarinda Medika Citra, dimana ada seseorang yang mengaku sebagai salah satu dokter yang mengatasnamakan rumah sakit menelpon salah satu orang tua pasien yang dirawat dengan maksud meminta orang tua dari pasien untuk mengirimkan sejumlah uang yang akan digunakan untuk membeli alat operasi untuk anak mereka yang sedang dirawat dirumah sakit dan orang tua pasien langsung mengirimkan uang yang diminta karena yang menelpon tersebut dapat menyebutkan secara rinci data dari pasien tersebut.

Pihak rumah sakit maupun klinik sangat menghawatirkan jika hal seperti ini sampai terjadi. Salah satu klinik di Tanjung Morawa yaitu Klinik Pratama Siti Rahmah mengenai data rekam medis pasien media penyimpanan yang masih digunakan adalah *database* sehingga data tersebut mudah sekali untuk dimanipulasi oleh oknum yang tidak berwenang karena belum memiliki sistem keamanan yang cukup baik maka membutuhkan solusi untuk bisa mengamankan data rekam medis pasien. Oleh karena itu, perlu dilakukan penyandian data tersebut kedalam bentuk yang tidak dapat dimengerti yaitu berupa kriptografi.

Kriptografi adalah cabang ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data untuk menjamin keamanan dan keutuhan dari suatu data [2]. Didalam kriptografi, terdapat banyak algoritma penyandian data seperti algoritma *Advanced Encryption Standard (AES)*. Algoritma *AES* adalah algoritma kriptografi simetrik yang dapat mengubah data sehingga berbeda dari bentuk aslinya dengan panjang kunci 128 bit. Proses dalam pengamanan data rekam medis ini yaitu dengan melakukan enkripsi dengan merubah data *text* atau pesan (*plaintext*) menjadi data sandi (*ciphertext*), dan dekripsi adalah merubah data sandi (*ciphertext*) menjadi data *text* atau pesan (*plaintext*) [3].

Keunggulan dari kriptografi dalam kemampuan penyandian yaitu dapat menyembunyikan informasi atau data dengan cara mengubah data asli menjadi sandi yang sulit ditemukan maknanya. Pengujian ini menggunakan algoritma *Advanced Encryption Standard (AES)* dengan panjang kunci 128 bit. Sehingga sangat cocok digunakan untuk keamanan pada data rekam medis pasien.

2. METODE PENELITIAN

Metode penelitian merupakan langkah atau cara tertentu yang digunakan oleh peneliti dalam rangka untuk mengumpulkan informasi agar hasil penelitian dapat memenuhi tujuan yang telah ditetapkan. Metode penelitian memberikan gambaran rancangan penelitian yang meliputi antara lain prosedur, langkah-langkah yang harus ditempuh, sumber data, dan dengan langkah apa data-data tersebut diperoleh dan selanjutnya diolah dan dianalisis. Berikut ini beberapa langkah-langkah yang dilakukan dalam penelitian ini yaitu sebagai berikut :

2.1 Teknik Pengumpulan Data

Untuk mendapatkan data dan informasi yang dibutuhkan terkait pengamanan data rekam medis di klinik pratama siti rahmah, terdapat beberapa teknik yang digunakan dalam penelitian ini yaitu sebagai berikut :

1. Observasi

Observasi merupakan teknik pengumpulan data secara langsung dengan tinjauan langsung ke klinik Pratama Siti Rahmah. Dalam penelitian ini yang diamati adalah masalah yang dihadapi selama ini terkait keamanan data rekam medis.

2. Wawancara

Wawancara ini dilakukan dengan tujuan untuk mendapatkan informasi yang tepat dan terpercaya, peneliti melakukan wawancara kepada dr.Roslitha Eryani dan para tenaga medis yang terlibat dalam proses pengolahan data rekam medis di klinik pratama siti rahmah.

Berikut ini merupakan data penelitian berupa data rekam medis klinik pratama siti rahmah, berdasarkan dari hasil observasi dan wawancara yang telah dilakukan, yaitu seperti yang terlihat di bawah ini:

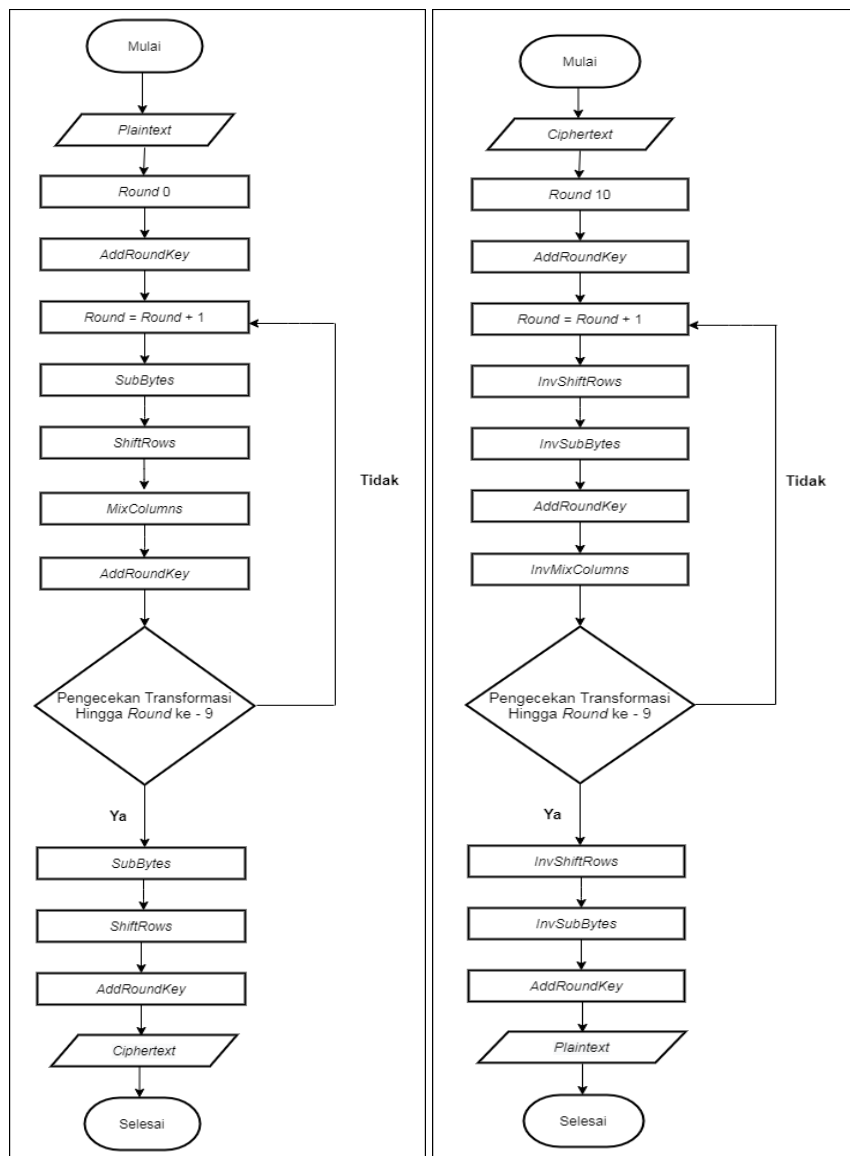
Tabel 2.1 Data Rekam Medis Klinik Pratama Siti Rahmah

No	ID Pasien	Data Rekam Medis
1.	1005	No Rekam Medis : 008729 Nama : DWI CAHYADI Umur : 18 Tahun Jenis Kelamin : Laki-laki Agama : Kristen Pekerjaan : Pelajar Alamat : Bangun Rejo Dusun V <i>Autonamnesis</i> : Demam, Nyeri kepala, Pilek (Dialami kurang lebih tiga hari) Diagnosa : Observasi Febris Obat dan Tindakan : Calortusin, Moxigra, Dextafen Tanggal Diagnosa : 26/10/2018 No Telepon : 0852-0000-23
2.	1110	No Rekam Medis : 123086 Nama : AHMAD WARSIM Umur : 49 Tahun Jenis Kelamin : Laki-laki Agama : Islam Pekerjaan : Karyawan Swasta PT. Mark Dynamics Indonesia Alamat : Bandar Labuhan Dusun I <i>Autonamnesis</i> : Nyeri panas di dada, Mual-mual, Batuk kering Diagnosa : Refluks Gastroesofagus (GERD) Obat dan Tindakan : Antasida, Simetikon, Proton pump inhibitors(PPI) Tanggal Diagnosa : 03/10/2018 No Telepon : 0823-0980-00
3.	1057	No Rmedis : 135045 Nama : RUDIANTO PRATAMA Umur : 38 Tahun Jenis Kelamin : Laki-laki Agama : Kristen Pekerjaan : Wiraswasta Alamat : Bangun Rejo Dusun VII <i>Autonamnesis</i> : Demam tinggi, Badan pegal, Diare Diagnosa : Thypoid Fever Obat dan Tindakan : Chloromycetin, Trimox, Ofloxacin, Azithromycin, Cotrimoxazole Tanggal Diagnosa : 13/10/2018 No Telepon : 0857-5060-001
4.	1028	No Rmedis : 150080 Nama : Zulfan Rifai Umur : 27 Tahun Jenis Kelamin : Laki-laki Agama : Islam Pekerjaan : Security Alamat : Tirta Deli <i>Autonamnesis</i> : Demam, Nyeri Dada, Sakit kepala, Mual-mual Diagnosa : Common cold, Dyspnea Obat dan Tindakan : Novaflox, Tera F, Dexanta, Gasela Tanggal Diagnosa : 03/07/2018 No Telepon : 0812-1011-123
5.	1019	No Rmedis : 180090 Nama : HALIMAH Umur : 45 Tahun Jenis Kelamin : Perempuan Agama : Islam Pekerjaan : - Alamat : Bandar Labuhan Bawah <i>Autonamnesis</i> : Badan pegal, Nyeri sendi, Demam, Mual-mual, Sakit Kepala, Bintik merah atau ruam Diagnosa : Danguue hemorrhagic fever(DHF) Obat dan Tindakan : Analgesik, Opname Tanggal Diagnosa : 31/07/2018 No Telepon : 0831-0080-908

Title of manuscript is short and clear, implies research results (First Author)

2.2 Flowchart Metode Advanced Encryption Standard 128bit

Flowchart merupakan langkah awal dalam pembuatan program, *flowchart* mempunyai bagan-bagan alur yang menggambarkan langkah-langkah penyelesaian suatu masalah.[4] *Flowchart* metode *Advanced Encryption Standard 128bit* merupakan keterangan yang lebih rinci tentang bagaimana prosedur yang dilakukan oleh suatu metode. *Flowchart* ini menggambarkan urutan dari suatu prosedur pemecahan masalah. Berikut ini merupakan *flowchart* enkripsi dan dekripsi metode *Advanced Encryption Standard 128bit*:



Gambar 2.1 Flowchart enkripsi dan dekripsi *advanced encryption standard 128bit*.

2.3 Penyelesaian Masalah dengan Metode *Advanced Encryption Standard 128bit*

Berikut ini adalah penyelesaian masalah mengenai pengamanan data Rekam Medis Di Klinik Pratama Siti Rahmah dengan metode *Advanced Encryption Standard 128bit* :

2.3.1 Ekspansi Kunci

Ekspansi kunci dilakukan dengan tujuan mendapatkan kunci ronde atau *roun key* yang akan digunakan untuk proses enkripsi dan dekripsi.[5] Pada algoritma *Advanced Encryption Standard*. Maksimal panjang kunci paada *Advanced Encryption Standard 128bit* adalah sebanyak 16 digit yang diperlukan adalah 10 kunci ronde yang diperoleh dari proses ekspansi. Kunci yang digunakan pada kasus ini adalah “REKAMMEDISRAHMAH”. Berikut adalah proses ekspansi kunci *advanced encryption standard* :

1. Urutkan *plaintext* kunci kedalam blok berukuran 128 bit (16 Kode ASCII), kemudian kunci diubah kedalam bentuk *Hexadecimal*.

R	E	K	A	M	M	E	D	I	S	R	A	H	M	A	H
52	45	4B	41	4D	4D	45	44	49	53	52	41	48	4D	41	48

2. Selanjutnya adalah mengubah kunci yang telah diubah ke dalam *state 4 x 4* seperti berikut:

52	45	4B	41
4D	4D	45	44
49	53	52	41
48	4D	41	48

→ RoundKey ke-0

3. Setelah itu, melakukan fungsi *RotWord*, yaitu dengan menggeser setiap bit pada kolom 4 ke atas 1 kali menggunakan *RoundKey ke-0* untuk menghasilkan *RoundKey ke-1*.

41
44
41
48

→

44
41
48
41

4. Setelah itu, melakukan substitusi hasil dari *RotWord* dengan nilai yang ada pada tabel S-Box Rijndael (*SubBytes*).

44
41
48
41

→

1B
83
52
83

5. Selanjutnya, untuk mendapatkan kolom pertama dari *RoundKey ke-1* adalah proses XOR antara kolom pertama dari *RoundKey ke-0* dan hasil dari *SubBytes* di XOR-kan dengan *Rcon (Round Constanta)*.

52	⊕	1B	⊕	01	=	48	Kolom ke-1
4D		83		00		CE	
49		52		00		1B	
48		83		00		CB	

6. Untuk mendapatkan nilai kolom selanjutnya dilakukan XOR antara kolom pertama (*Wi*) dengan kolom kedua dari *RoundKey ke-0*, kemudian untuk mendapatkan kolom berikutnya lakukan proses seperti kolom kedua.

45	⊕	48	=	0D	Kolom ke-2
4D		CE		83	
53		1B		48	
4D		CB		86	

$$\begin{array}{|c|c|} \hline 4B \\ \hline 45 \\ \hline 52 \\ \hline 41 \\ \hline \end{array} \oplus \begin{array}{|c|c|} \hline 0D \\ \hline 83 \\ \hline 48 \\ \hline 86 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 46 \\ \hline C6 \\ \hline 1A \\ \hline C7 \\ \hline \end{array} \quad \text{Kolom ke-3}$$

$$\begin{array}{|c|c|} \hline 41 \\ \hline 44 \\ \hline 41 \\ \hline 48 \\ \hline \end{array} \oplus \begin{array}{|c|c|} \hline 46 \\ \hline C6 \\ \hline 1A \\ \hline C7 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 07 \\ \hline 82 \\ \hline 5B \\ \hline 8F \\ \hline \end{array} \quad \text{Kolom ke-4}$$

7. Dari seluruh proses yang telah dilakukan seperti di atas, maka didapatkanlah *RoundKey* ke-1, yaitu :

48	0D	46	07
CE	83	C6	82
1B	48	1A	5B
CB	86	C7	8F

Untuk mendapatkan *RoundKey* ke-2 sampai dengan *RoundKey* ke-10, proses di atas diulang sebanyak 10 kali. Di bawah ini merupakan hasil ekspansi kunci dari setiap *round* yang akan digunakan untuk proses enkripsi dan dekripsi:

<i>RoundKey</i> ke-1				<i>RoundKey</i> ke-2				...	<i>RoundKey</i> ke-10			
48	0D	46	07	59	54	12	15		99	D6	05	C0
CE	83	C6	82	F7	74	B2	30		CA	3C	14	C4
1B	48	1A	5B	68	20	3A	61		0C	95	E2	7D
CB	86	C7	8F	0E	88	4F	C0		DF	EC	9A	BD

2.3.2 Enkripsi

Proses enkripsi pada algoritma *Advanced Encryption Standard* terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns* dan *AddRoundKey*[6] proses enkripsi akan dilakukan pada *record database* data Rekam Medis Klinik Pratama Siti Rahmah. *Plaintext* yang dienkripsi adalah “RUDIANTO PRATAMA”, dengan proses enkripsi seperti berikut ini:

1. *Plaintext* diurutkan kedalam blok dan diubah kedalam bentuk bilangan *hexadecimal*.

R	U	D	I	A	N	T	O		P	R	A	T	A	M	A
52	55	44	49	41	4E	54	4F	20	50	52	41	54	41	4D	41

2. *Plaintext* yang diubah ke *hexadecimal* yang telah disusun 16 *byte* pertama dibentuk kedalam *state* 4 x 4.

52	55	44	49
41	4E	54	4F
20	50	52	41
54	41	4D	41

3. Selanjutnya proses *AddRoundKey*, pada proses ini XOR-kan *plaintext* dengan *RoundKey* ke-0.

$$\begin{array}{|c|c|c|c|} \hline 52 & 55 & 44 & 49 \\ \hline 41 & 4E & 54 & 4F \\ \hline 20 & 50 & 52 & 41 \\ \hline 54 & 41 & 4D & 41 \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|} \hline 52 & 45 & 4B & 41 \\ \hline 4D & 4D & 45 & 44 \\ \hline 49 & 53 & 52 & 41 \\ \hline 48 & 4D & 41 & 48 \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline 00 & 10 & 0F & 08 \\ \hline 0C & 03 & 11 & 0B \\ \hline 69 & 03 & 00 & 00 \\ \hline 1C & 0C & 0C & 09 \\ \hline \end{array}$$

4. Hasil dari *AddRoundKey* diatas akan menjadi *round* ke-1 untuk diproses dengan 4 transformasi, yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*.

a. Transformasi pertama yaitu *SubBytes*, pada tahap ini setiap *byte* akan ditukar dengan tabel *S-Box*.

00	10	0F	08
0C	03	11	0B
69	03	00	00
1C	0C	0C	09

 \longrightarrow

63	CA	76	30
FE	7B	82	2B
F9	7B	63	63
9C	FE	FE	01

b. Transformasi berikutnya adalah *ShiftRows*, baris pertama tidak ada pergeseran, baris kedua dilakukan pergeseran 1 *byte*, pada baris ketiga digeser 2 *byte* dan baris keempat digeser 3 *byte* ke kiri.

63	CA	76	30
FE	7B	82	2B
F9	7B	63	63
9C	FE	FE	01

 \longrightarrow

63	CA	76	30
7B	82	2B	FE
63	63	F9	7B
01	9C	FE	FE

c. Selanjutnya adalah proses *MixColumns*, dimana proses ini akan melakukan perkalian antara *polynomial* tetap dengan *state* hasil dari *ShiftRows*.

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

 \times

63	CA	76	30
7B	82	2B	FE
63	63	F9	7B
01	9C	FE	FE

 $=$

29	ED	96	FC
31	EC	CE	A4
DD	31	AD	21
BF	87	AF	32

d. Tranformasi akhir dari *round* ke-1 adalah *AddRoundKey*, hasil dari *MixColumns* akan di XOR-kan dengan *RoundKey* ke-1, seperti dibawah ini.

29	ED	96	FC
31	EC	CE	A4
DD	31	AD	21
BF	87	AF	32

 \oplus

48	0D	46	07
CE	83	C6	82
1B	48	1A	5B
CB	86	C7	8F

 $=$

61	E0	D0	FB
FF	6F	08	26
C6	79	B7	7A
74	01	68	BD

Proses diatas akan diulangi untuk *round* ke-2 sampai dengan *round* ke-10. Namun, pada *round* ke 10 transformasi *MixColumns* tidak lagi dilakukan. Berikut hasil transformasi proses enkripsi:

Round ke-2

<i>SubBytes</i>	<i>ShiftRows</i>	<i>MixColumn</i>																																																
<table border="1" style="width: 100%;"> <tr><td>EF</td><td>E1</td><td>70</td><td>0F</td></tr> <tr><td>A8</td><td>30</td><td>F7</td><td>16</td></tr> <tr><td>A9</td><td>DA</td><td>B4</td><td>B6</td></tr> <tr><td>7A</td><td>92</td><td>7C</td><td>45</td></tr> </table>	EF	E1	70	0F	A8	30	F7	16	A9	DA	B4	B6	7A	92	7C	45	<table border="1" style="width: 100%;"> <tr><td>EF</td><td>E1</td><td>70</td><td>0F</td></tr> <tr><td>16</td><td>A8</td><td>30</td><td>F7</td></tr> <tr><td>B4</td><td>B6</td><td>A9</td><td>DA</td></tr> <tr><td>92</td><td>7C</td><td>45</td><td>7A</td></tr> </table>	EF	E1	70	0F	16	A8	30	F7	B4	B6	A9	DA	92	7C	45	7A	<table border="1" style="width: 100%;"> <tr><td>F5</td><td>C1</td><td>2A</td><td>D7</td></tr> <tr><td>3E</td><td>66</td><td>3E</td><td>A7</td></tr> <tr><td>80</td><td>D3</td><td>70</td><td>A1</td></tr> <tr><td>DF</td><td>ED</td><td>2B</td><td>3B</td></tr> </table>	F5	C1	2A	D7	3E	66	3E	A7	80	D3	70	A1	DF	ED	2B	3B
EF	E1	70	0F																																															
A8	30	F7	16																																															
A9	DA	B4	B6																																															
7A	92	7C	45																																															
EF	E1	70	0F																																															
16	A8	30	F7																																															
B4	B6	A9	DA																																															
92	7C	45	7A																																															
F5	C1	2A	D7																																															
3E	66	3E	A7																																															
80	D3	70	A1																																															
DF	ED	2B	3B																																															
<i>RoundKey ke-2</i>	<i>AddRoundKey</i>																																																	
<table border="1" style="width: 100%;"> <tr><td>59</td><td>54</td><td>12</td><td>15</td></tr> <tr><td>F7</td><td>74</td><td>B2</td><td>30</td></tr> <tr><td>68</td><td>20</td><td>3A</td><td>61</td></tr> <tr><td>0E</td><td>88</td><td>4F</td><td>C0</td></tr> </table>	59	54	12	15	F7	74	B2	30	68	20	3A	61	0E	88	4F	C0	<table border="1" style="width: 100%;"> <tr><td>AC</td><td>95</td><td>38</td><td>C2</td></tr> <tr><td>C9</td><td>12</td><td>8C</td><td>97</td></tr> <tr><td>E8</td><td>F3</td><td>4A</td><td>C0</td></tr> <tr><td>D1</td><td>65</td><td>64</td><td>FB</td></tr> </table>	AC	95	38	C2	C9	12	8C	97	E8	F3	4A	C0	D1	65	64	FB																	
59	54	12	15																																															
F7	74	B2	30																																															
68	20	3A	61																																															
0E	88	4F	C0																																															
AC	95	38	C2																																															
C9	12	8C	97																																															
E8	F3	4A	C0																																															
D1	65	64	FB																																															

.....

Round ke-10

<i>SubBytes</i>	<i>ShiftRows</i>	<i>RoundKey ke-10</i>																																																
<table border="1" style="width: 100%;"> <tr><td>DA</td><td>BE</td><td>FA</td><td>2B</td></tr> <tr><td>AD</td><td>C2</td><td>85</td><td>49</td></tr> <tr><td>A8</td><td>92</td><td>CC</td><td>50</td></tr> <tr><td>31</td><td>5A</td><td>DA</td><td>8E</td></tr> </table>	DA	BE	FA	2B	AD	C2	85	49	A8	92	CC	50	31	5A	DA	8E	<table border="1" style="width: 100%;"> <tr><td>DA</td><td>BE</td><td>FA</td><td>2B</td></tr> <tr><td>C2</td><td>85</td><td>49</td><td>AD</td></tr> <tr><td>CC</td><td>50</td><td>A8</td><td>92</td></tr> <tr><td>8E</td><td>31</td><td>5A</td><td>DA</td></tr> </table>	DA	BE	FA	2B	C2	85	49	AD	CC	50	A8	92	8E	31	5A	DA	<table border="1" style="width: 100%;"> <tr><td>99</td><td>D6</td><td>05</td><td>C0</td></tr> <tr><td>CA</td><td>3C</td><td>14</td><td>C4</td></tr> <tr><td>0C</td><td>95</td><td>E2</td><td>7D</td></tr> <tr><td>DF</td><td>EC</td><td>9A</td><td>BD</td></tr> </table>	99	D6	05	C0	CA	3C	14	C4	0C	95	E2	7D	DF	EC	9A	BD
DA	BE	FA	2B																																															
AD	C2	85	49																																															
A8	92	CC	50																																															
31	5A	DA	8E																																															
DA	BE	FA	2B																																															
C2	85	49	AD																																															
CC	50	A8	92																																															
8E	31	5A	DA																																															
99	D6	05	C0																																															
CA	3C	14	C4																																															
0C	95	E2	7D																																															
DF	EC	9A	BD																																															

AddRoundKey

43	68	FF	EB
08	B9	5D	69
C0	C5	4A	EF
51	DD	C0	67

Hasil dari proses enkripsi yaitu: 4368FFEB08B95D69C0C54AEF51DDC067

2.3.3 Dekripsi

Proses dekripsi merupakan kebalikan dari proses enkripsi, proses dekripsi menggunakan transformasi *invers*[7]. Proses dekripsi ini dilakukan untuk mengembalikan *text* atau *record* yang telah dienkripsi menjadi *plaintext* kembali. Proses transformasi pada dekripsi dalam algoritma *advanced encryption standard* adalah *InvSubBytes*, *InvShiftRows*, *InvMixColumns*, dan *AddRoundKey*.

Berikut adalah proses dekripsi dari chipertext “4368FFEB08B95D69C0C54AEF51DDC067”:

Melakukan proses XOR antara chipertext dengan RoundKey ke-10.

43	68	FF	EB
08	B9	5D	69
C0	C5	4A	EF
51	DD	C0	67

 \oplus

99	D6	05	C0
CA	3C	14	C4
0C	95	E2	7D
DF	EC	9A	BD

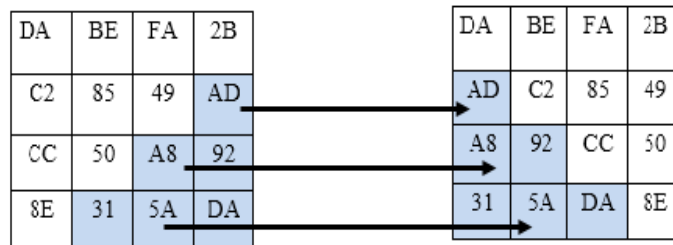
 $=$

DA	BE	FA	2B
C2	85	49	AD
CC	50	A8	92
8E	31	5A	DA

1. Karena pada *round* ke-1 dalam proses dekripsi, tidak melakukan proses *InvMixColumns*. Maka proses selanjutnya adalah melakukan transformasi *InvShiftRows*.

Round ke-1

InvShiftRows



2. Kemudian, lakukan proses *InvSubBytes*. Untuk S-Box *InvSubBytes* berbeda dengan S-BOX *SubBytes* karena telah dilakukan *invers* namun, cara kerjanya sama.

DA	BE	FA	2B
AD	C2	85	49
A8	92	CC	50
31	5A	DA	8E

 \rightarrow

7A	5A	14	0B
18	A8	67	A4
6F	74	27	6C
2E	46	7A	E6

3. Selanjutnya, lakukan operasi XOR antara *InvSubBytes* dengan *RoundKey* ke- 9 untuk transformasi *AddRoundKey*.

7A	5A	14	0B
18	A8	67	A4
6F	74	27	6C
2E	46	7A	E6

 \oplus

DF	4F	D3	C5
11	F6	28	D0
C0	99	77	9F
79	33	76	27

 $=$

A5	15	C7	CE
09	5E	4F	74
AF	ED	50	F3
57	75	0C	C1

4. Selanjutnya, melakukan proses transformasi antara hasil *AddRoundKey* dengan dot product dengan mengikuti aturan *irreducible polynomial*.

$$\begin{array}{|c|c|c|c|} \hline 0E & 0B & 0D & 09 \\ \hline 09 & 0E & 0B & 0D \\ \hline 0D & 09 & 0E & 0B \\ \hline 0B & 0D & 09 & 0E \\ \hline \end{array} \times \begin{array}{|c|c|c|c|} \hline A5 & 15 & C7 & CE \\ \hline 09 & 5E & 4F & 74 \\ \hline AF & ED & 50 & F3 \\ \hline 57 & 75 & 0C & C1 \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline 0C & 5F & 88 & F1 \\ \hline FF & 9E & 48 & 27 \\ \hline AE & 1A & AC & C7 \\ \hline 09 & 08 & B8 & 99 \\ \hline \end{array}$$

Proses di atas akan diulangi untuk mendapatkan hasil transformasi *round* ke-2 sampai dengan *round* ke-10, seperti yang di bawah ini :

Round ke-2

<i>InvShiftRows</i>				<i>InvSubBytes</i>				<i>RoundKey ke-8</i>			
0C	5F	88	F1	81	84	97	2B	85	90	9C	16
27	FF	9E	48	3D	7D	DF	D4	8A	E7	DE	F8
AC	C7	AE	1A	AA	31	BE	43	11	59	EE	E8
08	B8	99	09	BF	9A	F9	40	3E	4A	45	51
<i>AddRoundKey</i>				<i>InvMixColumn</i>							
04	14	0B	3D	1E	65	FF	F5				
B7	9A	01	2C	DA	CB	F6	49				
BB	68	50	AB	A8	75	73	2E				
81	D0	BC	11	E5	ED	9C	39				

.....

Round ke-10

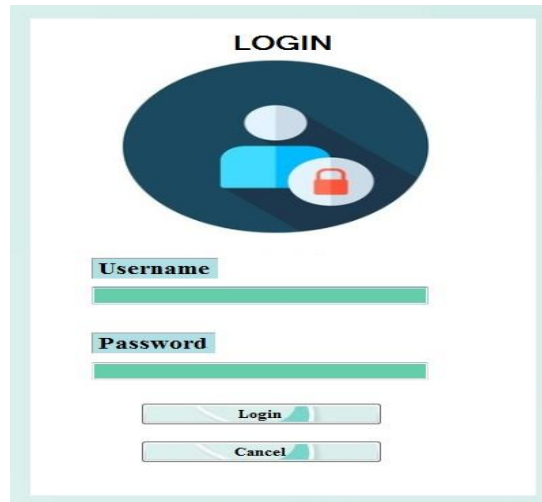
<i>InvShiftRows</i>				<i>InvSubBytes</i>				<i>RoundKey ke-0</i>			
63	CA	76	30	00	10	0F	08	52	45	4B	41
FE	7B	82	2B	0C	03	11	0B	4D	4D	45	44
F9	7B	63	63	69	03	00	00	49	53	52	41
9C	FE	FE	01	1C	0C	0C	09	48	4D	41	48
<i>AddRoundKey</i>											
52	55	44	49								
41	4E	54	4F								
20	50	52	41								
54	41	4D	41								

Hasil dari proses dekripsi yaitu: 52554449414E544F2050524154414D41

3. ANALISA DAN HASIL

3.1 Tampilan Form Login

Tampilan menu login adalah tampilan untuk masuk ke menu utama. *User* harus melakukan login terlebih dahulu dengan cara menginput *username* dan *password* dengan benar sesuai dengan *database*. Berikut ini adalah tampilan menu *login* :

Gambar 3.1 Tampilan *form Login*

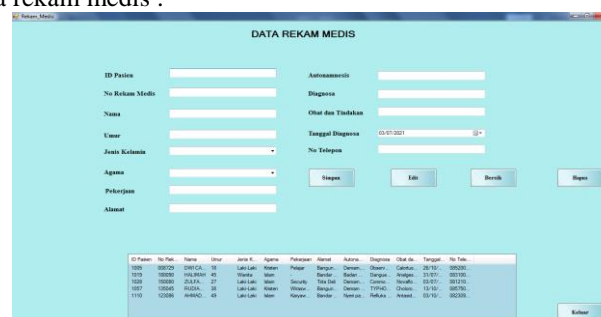
3.2 Tampilan *Form Menu Utama*

Tampilan *form* menu utama adalah tampilan awal sistem untuk melakukan pengolahan data dalam pengamanan data rekam medis. Berikut ini adalah tampilan menu utama :

Gambar 3.2 Tampilan *Form Menu Utama*

3.3 Tampilan *Form Data Rekam Medis*

Tampilan *form* menu data rekam medis adalah *form* untuk menginput data rekam medis. Berikut ini adalah tampilan *form* data rekam medis :

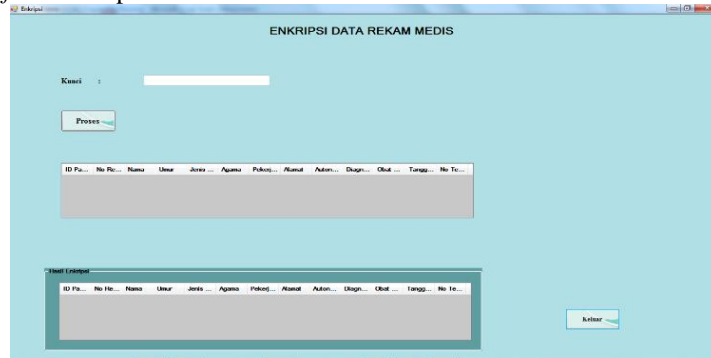


ID Pasien	No Rekam Medis	Nama	Umur	Jenis Kelamin	Agama	Pekerjaan	Aliases
1001	100001	DIANA CA	18	Laki-Laki	Kristen	Pegawai	Banyuwangi
1002	100002	SITI RAHMAH	45	Wanita	Islam	Bekerja	Banyuwangi
1003	100003	DIANA K	27	Laki-Laki	Islam	Swasta	Tela Dua
1004	100004	INDRA	25	Laki-Laki	Islam	Bekerja	Banyuwangi
1110	100005	INDRA	45	Laki-Laki	Islam	Karyawan	Banyuwangi

Gambar 3.3 Tampilan *Form Data Rekam Medis*

3.4 Tampilan Form Enkripsi

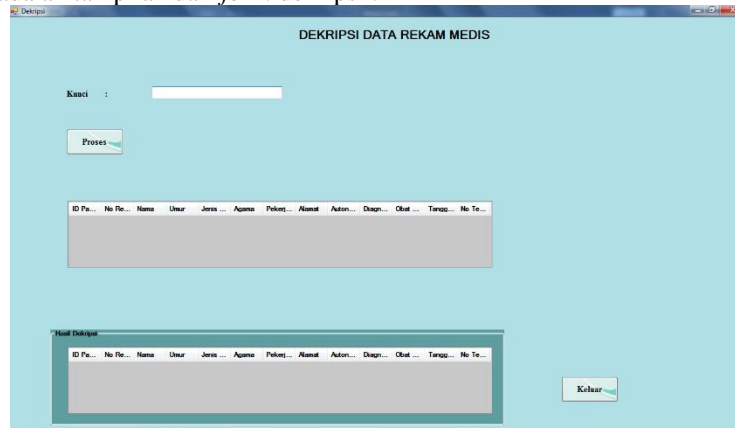
Form enkripsi digunakan untuk melakukan proses penyandian pada data rekam medis. Berikut ini adalah tampilan dari form enkripsi :



Gambar 3.4 Tampilan Hasil Encrypt

3.5 Tampilan Form Dekripsi

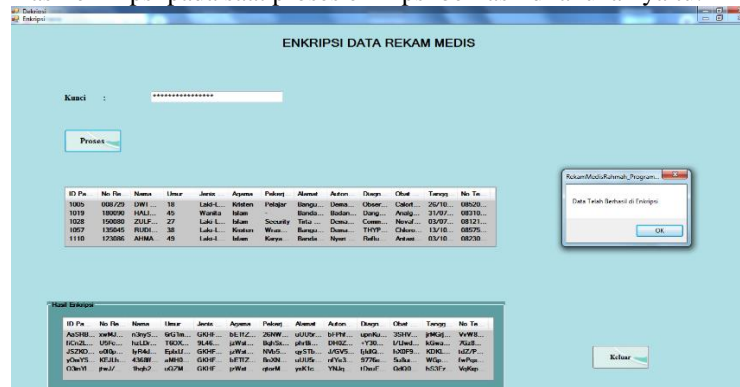
Form dekripsi digunakan untuk mengembalikan data yang sebelumnya sudah dienkripsi agar dapat dibaca. Berikut ini adalah tampilan dari form dekripsi :



Gambar 3.5 Tampilan Form Dekripsi

3.6 Tampilan Hasil Enkripsi

Berikut adalah hasil enkripsi pada saat proses enkripsi berhasil dilakukan yaitu:

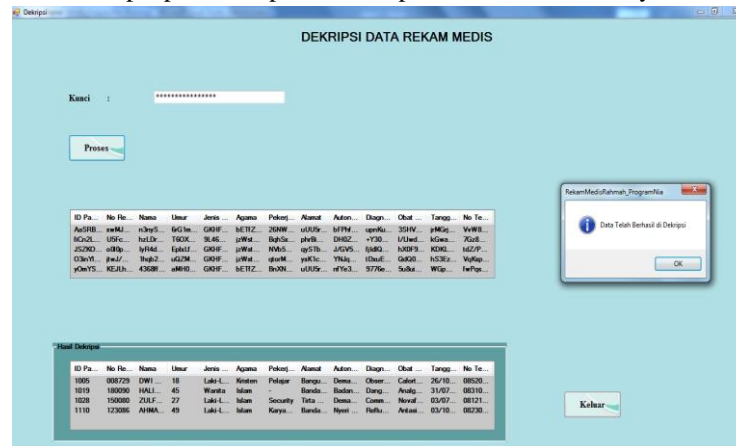


Gambar 3.6 Tampilan Hasil Enkripsi

3.7 Tampilan Hasil Dekripsi

Title of manuscript is short and clear, implies research results (First Author)

Berikut adalah hasil dekripsi pada saat proses dekripsi berhasil dilakukan yaitu:



Gambar 3.7 Tampilan Hasil Dekripsi

4. KESIMPULAN

Kesimpulan yang dapat diambil dalam pembuatan sistem keamanan data rekam medis pada Klinik Pratama Siti Rahmah dengan menggunakan metode *Advanced Encryption Standard* 128bit antara lain:

1. Dalam penerepan metode *Advanced Encryption Standard* 128bit dapat mempermudah dalam menjaga keamanan dan kerahasiaan pada data rekam medis dari orang yang tidak bertanggung jawab.
2. Berdasarkan hasil perancangan, sistem yang telah dibangun dengan menggunakan aplikasi *Visual Basic 2010* dan *Microsoft Access 2016* dengan Algoritma *Advanced Encryption Standard 128 bit*, sistem ini mampu mengamankan Data Rekam Medis pada Klinik Pratama Siti Rahmah.
3. Berdasarkan pengujian sistem yang telah dibangun dengan algoritma *Advanced Encryption Standard* dapat mempermudah mengamankan data rekam medis dengan baik, semua data *plaintext* yang disisipkan akan diubah menjadi enkripsi atau data yang tidak bisa dimengerti dengan cara memasukkan kunci dengan benar.

UCAPAN TERIMA KASIH

Pada kesempatan ini penulis mengucapkan banyak terimakasih kepada kedua orang tua yang telah banyak memberikan dukungan moril dan materil, tidak terkecuali doa yang senantiasa dipanjatkan sehingga penulis dapat menyelesaikan penelitian ini.




Penyusunan jurnal ini juga tidak terlepas dari bantuan berbagai pihak. Oleh karena itu dengan segala kerendahan hati, diucapkan terimakasih yang sebesar-besarnya kepada: Bapak Nurcahyo Budi Nugroho, S.Kom., M.Kom selaku Dosen Pembimbing I, kepada Ibu Sri Murniyanti, S.S., M.M selaku Dosen Pembimbing II yang telah banyak membantu dalam memberikan arahan dan bimbingan.

REFERENSI

- [1] H. A. Kartika, A. Kusyanti, and M. Data, "Implementasi Algoritme SPECK dan SHA-3 Pada Database Rekam Medik," vol. 2, no. 12, pp. 6942–6951, 2018.
- [2] R. Nuari, N. Ratama, J. T. Informatika, F. Teknik, and U. Pamulang, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," vol. 1, no. 2, pp. 37–44, 2020.
- [3] J. Prayudha, "Implementasi Keamanan Data Gaji Karyawan Pada PT . Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," vol. 18, no. 2, 2019.

- [4] D'Arcy Wentworth Thompson, “*濟無*No Title No Title No Title,” *Angew. Chemie Int. Ed.* 6(11), 951–952., pp. 12–46, 1967.
- [5] A. Rachman, “Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES),” vol. 3, no. 2, pp. 112–115, 2018.
- [6] A. S. A.Prajuhana Putra, Herfina, S.Mariana, “Implementasi Algoritma AES (Advanced Encryption Standard) Rijndael Pada Aplikasi Keamanan Data,” vol. 1, pp. 46–51, 2020.
- [7] L. Mustika, “Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 148, 2020, doi: 10.30865/jurikom.v7i1.1943.

BIBLIOGRAFI PENULIS

	<p>Nama : Nur Nia Suci Tempat/Tgl : Bangun Rejo, 27 Mei 1999 Alamat : Jl. Limau Mungkur Kel. Bangun Rejo Dusun IV Agama : Islam Jenis Kelamin : Perempuan No.Hp : 0857-6184-4973 Bidang Keilmuan : Kriptografi dan Desain Grafis E-mail : nurniasuci47@gmail.com</p>
	<p>Nama : Nurcahyo Budi Nugroho, S.Kom., M.Kom Tempat/Tgl : Temanggung, 30 Maret 1982 Alamat : - Agama : Islam Jenis Kelamin : Laki-Laki No.Hp : 0858-3151-1117 Prestasi Dosen : - Bidang Keilmuan : Algoritma & Pemrograman I, Pemrograman Web, Pemrograman Mobile, Pengolahan Citra, Keamanan Komputer, Jaringan Syaraf Tiruan Email : nurcahyobn@gmail.com</p>
	<p>Nama : Sri Murniyanti, S.S., M.M Tempat/Tgl : Medan, 3 Januari 1972 Alamat : - Agama : Islam Jenis Kelamin : Perempuan No.Hp : 0821-6524-5043 Prestasi Dosen : - Bidang Keilmuan : PMB, Teknik Pemasaran, Technopreneur Email : Srimurnianti21@gmail.com</p>