
E-Security Untuk Member Data Collection Administration System Menggunakan Metode Advanced Encryption Standard (AES)

Lutfita Andini ¹, Azanuddin ², Ita Mariami ³

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

²Program Studi Sistem Komputer, STMIK Triguna Dharma

Article Info

Article history:

Received Jul 12th, 2020

Revised Jul 20th, 2020

Accepted Jul 30th, 2020

Keyword:

Keamanan Data

Database

Advanced Encryption Standard

ABSTRACT

RAPI 0201 Kota Medan adalah sebuah organisasi yang bergerak dalam penyelenggaraan telekomunikasi radio yang memanfaatkan teknologi komputer khususnya terkait database sehingga setiap informasi dari setiap anggota tersimpan dalam bentuk arsip elektronik data administrasi yang bersifat rahasia dan hanya dikelola oleh Admin atau Sekertaris Wilayah RAPI. Permasalahan yang ada di RAPI 0201 yaitu arsip elektronik belum memiliki sistem keamanan, sehingga memungkinkan adanya pihak yang tidak bertanggung jawab untuk memodifikasi dan melakukan pencurian terhadap data-data tersebut. Solusi untuk membantu organisasi RAPI 0201 Kota Medan dalam mengamankan database data administrasi dapat dilakukan dengan membuat sistem keamanan kriptografi yang mempelajari teknik matematika mengenai keamanan data seperti kerahasiaan, integritas, dan otentikasi. Dalam penyelesaian masalah terkait pengamanan database data administrasi anggota metode yang digunakan adalah algoritma advanced encryption standard yang merupakan standard kriptografi simetri dengan panjang kunci yang digunakan yaitu 128 bit dengan kemungkinan tahan terhadap serangan exhaustive key search.

Copyright © 2020 STMIK Triguna Dharma.

All rights reserved.

Corresponding Author:

Nama : Lutfita Andini

Program Studi : Sistem Informasi

STMIK Triguna Dharma

Email : lintangkasa@gmail.com

1. PENDAHULUAN

Komunikasi adalah suatu kebutuhan fundamental bagi seseorang dalam hidup bermasyarakat, sebab tanpa adanya komunikasi masyarakat tidak akan terbentuk. Salah satu bentuk perkembangan komunikasi adalah telekomunikasi menggunakan radio[1]. RAPI adalah organisasi yang telah dilegalkan oleh pemerintah Indonesia untuk mengorganisir penyelenggaraan telekomunikasi radio. Karena bersifat nasional RAPI memiliki anggota yang tersebar diseluruh pelosok negeri. Untuk mempermudah proses pendataan anggota, RAPI memanfaatkan teknologi komputer sehingga setiap informasi dari setiap anggota tersimpan dalam bentuk data administrasi.

Member Data Collection Administration System adalah sebuah sistem pengelola data administrasi yang di dalamnya terdapat serangkaian kegiatannya berupa pengumpulan, pengelolaan, penyimpanan, dan penyajian data keanggotaan organisasi agar tujuan yang dicapai dapat hasil yang optimal. Data Administrasi Anggota Rapi adalah salah satu data yang bersifat rahasia dan tersimpan di dalam arsip elektronik, hanya pihak-pihak tertentu saja yang dapat menerima dan membaca data tersebut disebabkan, beberapa data bersifat pribadi. Namun hal ini, tidak terlepas dari adanya ancaman manipulasi dan pencurian data oleh pihak-pihak yang tidak berwenang, sehingga pentingnya pengamanan pada data administrasi anggota RAPI untuk menjaga keakuratan dan kerahasiaan data.

Dalam penerapan keamanan data digital dapat dilakukan dengan beberapa cara, seperti dengan menerapkan teknik penyamaran data (*cryptology*). Kriptografi adalah bidang yang mempelajari teknik atau ilmu matematika, kriptografi berkaitan dengan keamanan informasi, kerahasiaan data, integritas data, dan otentikasi data[2]. Dalam cabang ilmu kriptografi, terdapat dua proses yang sangat penting harus dilakukan, yaitu: proses enkripsi dan dekripsi. Proses enkripsi adalah proses mengubah informasi menjadi bentuk lain yang tidak dapat dipahami menggunakan algoritma tertentu, sedangkan proses dekripsi adalah proses memulihkan informasi yang dienkripsi sehingga dapat dipahami kembali[3].

Salah satu algoritma pada kriptografi adalah AES (*Advanced Encryption Standard*) yang termasuk dalam kelompok block cipher yang dapat mengenkripsi atau menyandikan dan dekripsi sebuah informasi. AES adalah sebuah algoritma *block cipher* dengan karakteristik sebagai berikut: Biasanya menggunakan sistem permutasi dan penggantian (P-Box dan S-Box)[4]. Ada tiga jenis AES berdasarkan panjang kunci pada umumnya, yaitu AES-128, AES-192, dan AES- 256. Algoritma AES memiliki panjang kunci paling sedikit yaitu 128 bit dan akan membentuk susunan matriks berukuran 4×4 . Dengan panjang kunci 128 bits maka terdapat sebanyak $2^{128} = 3,4 \times 10^{38}$ kemungkinan kunci membuat AES tetap tahan terhadap serangan *exhaustive key search* dengan teknologi yang ada saat ini data masukan akan dibagi dengan 8 bit[5].

2. METODE PENELITIAN

Metode penelitian merupakan langkah-langkah yang di lakukan untuk mengumpulkan data atau informasi yang dibutuhkan oleh seorang pengembang perangkat lunak (*Software*) sebagai tahapan serta gambaran penelitian yang akan dibuat. Berikut adalah metode dalam penelitian ini yaitu :

2.1 Teknik Pengumpulan Data

Untuk mendapatkan data dan informasi yang dibutuhkan terkait pengamanan data administrasi anggota pada organisasi RAPI 0201 Kota Medan, ada 2 tahapan yang dilakukan dalam penelitian ini adalah sebagai berikut:

1. Observasi

Studi observasi merupakan teknik pengumpulan data secara langsung di RAPI 0201 Kota Medan selama ± 3 bulan terakhir pada tanggal 02 November 2020 – 30 Januari 2021 terhadap kejadian-kejadian, perilaku, dan hal-hal lain yang diperlukan dalam mendukung penelitian yang sedang berlangsung.

2. Wawancara

Wawancara ini dilakukan dengan tujuan untuk mendapatkan informasi yang tepat dan terpercaya dengan pihak – pihak yang memiliki wewenang seperti pada Sekretaris Wilayah RAPI 0201 Kota Medan, dengan mengajukan beberapa pertanyaan terkait kendala – kendala yang terjadi pada sistem informasi mengenai administrasi keanggotaan organisasi RAPI.

Berikut ini merupakan data penelitian berupa data administrasi anggota organisasi RAPI 0201 Kota Medan, berdasarkan dari hasil observasi dan wawancara yang telah dilakukan, yaitu seperti yang terlihat di bawah ini:

Tabel 2.1 Data Anggota Administrasi RAPI 0201 Kota Medan

No	Nama	Nomor NIK	Tpt/Tgl. Lahir	Agama	Jenis Kelamin	Alamat	Gol Darah	No HP / Email	Kontribusi Daerah	Kontribusi Nasional	E - KTP
1	Indra Gunawan	1271112010710006	P. Siantar / 20 Oktober 1971	Islam	L	Jl.Karya Jaya, Gg.Eka Lembah, Lingk-II, 20144	A			Rp. 57.700,-	image/ktp.jpg
2	Dudi Rahmadiansyah	1271212108780001	Bunut / 21 Agustus 1978	Islam	L	Komp. Puri Zhara No.C02 Kelurahan Kemenangan Tani, 20136	B	081361652006/e.ktasumut@gmail.com	Rp. 115.000,-	Rp. 57.700,-	image/ktpdudi.jpg
3	Juliani	1271115707690001	Medan / 17 Juli 1969	Islam	P	Jalan Eka Suka VII No 6A Lingkungan XII Medan Kelurahan Gedung Johor ,20144	AB	082160559174 / e.ktasumut@gmail.com	Rp. 115.000,-	Rp. 57.700,-	image/ktpjuliani.jpg
4	Sugihartono S,Sos.,M.Si	1271130703620002	Medan / 7 Maret 1962	Islam	L	Jl. Tuar 11 no. 13. Blok XI. Kel. Besar, Medan Labuhan,20253	AB	082272401962 / sugihartonososmsi@gmail.com			image/ktpsugi.jpg
5	Hanafi Maksum	1207261006740019	Medan / 10 Juni 1974	Islam	L	Jalan Denai Gg.Rukun No.16 Desa Tegal Sari I, 20216		e.ktasumut@gmail.com		Rp. 57.000,-	image/ktphanafi.jpg

2.2 Flowchart Metode Advanced Encryption Standard 128bit

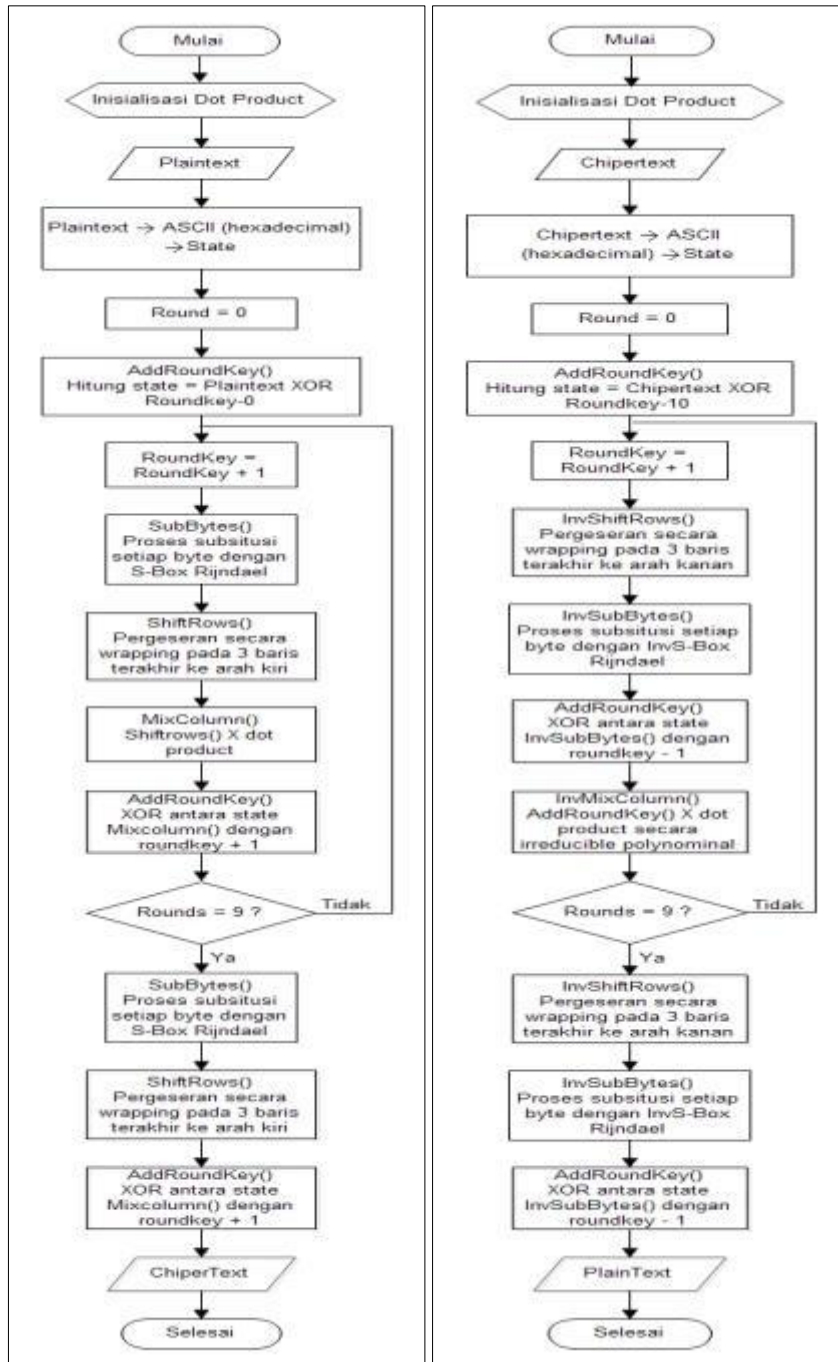
Langkah - langkah menggunakan algoritma AES 128 bit dalam menyelesaikan masalah terkait pengamanan *database*, terlihat seperti dibawah ini.

Kunci ronde dibutuhkan untuk setiap ronde transformasi penyandian AES. *Key schedule* adalah proses untuk mendapatkan ekspansi kunci, dimana N_b ($N_r + 1$) *word*, sehingga AES 128 bit menghasilkan $4(10+1) = 40$ *word* = 44×32 bit = 1408 bit *subkey*. *Subkey* ini diperlukan karena setiap *round* merupakan suatu inisial dari N_b *word* untuk $N_r=0$, N_b untuk $N_r=1$, dan 3 untuk $N_r=2, \dots$ dari operasi ini akan didapatkan *key schedule* yang berisi *array linier 4 byte word* (w_i), $0 = i$ ($N_r + 1$)

Langkah-langkah yang terdapat pada proses ekspansi kunci AES 128bit adalah seperti berikut ini:

1. *RotWord*, yaitu mengambil masukan empat *byte* kata [a_0, a_1, a_2, a_3] dan melakukan perputaran permutasi menjadi [a_1, a_2, a_3, a_0].
2. *SubWord*, mensubsitisi hasil *RotWord* dengan *S-Box Rijndael*.
3. *Rcon*, yaitu melakukan operasi XOR antara kolom pertama dari *RoundKey* ke-0 dengan hasil *SubWord* dan *Round Constanta (Rcon)*[6].

Proses Enkripsi adalah proses mengubah pesan (*plaintext*) menjadi pesan yang disandikan sehingga pihak lain tidak dapat membaca isi pesan. Sedangkan proses Dekripsi adalah proses pengembalian *chipertext* menjadi pesan awal yang dapat dibaca. Secara keseluruhan algoritma dekripsi merupakan kebalikan dari algoritma enkripsi, yang berupa transformasi *invers*. Proses enkripsi dan dekripsi dapat digambarkan seperti berikut[7]:



Gambar 2.2 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 administrasi RAPI 0201 Kota Medan dengan metode *Advanced Encryption Standard* 128bit :

2.3.1 Ekspansi Kunci

Ekspansi kunci dibutuhkan untuk proses enkripsi dan deskripsi pada tahapan *AddRoundKey*. Maksimal panjang kunci pada *Advanced Encryption Standard* 128 bit adalah 16 digit yang membutuhkan adalah 10 kunci ronde. Kunci yang digunakan pada kasus ini adalah “RAPI 0201 KMEDAN”. Berikut adalah proses ekspansi kunci *advanced encryption standard* :

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

R	A	P	I		0	2	0	1		K	M	E	D	A	N
52	41	50	49	20	30	32	30	31	20	4B	4D	45	44	41	4E

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

52	20	31	45
41	30	20	44
50	32	4B	41
49	30	4D	4E

→ RoundKey ke-0

- 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.

45	44
44	41
41	4E
4E	45

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

44	1B
41	83
4E	2F
45	6E

- 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
41	83	00	C2	
50	2F	00	7F	
49	6E	00	27	

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

20	48	68	Kolom ke-2
30	C2	F2	
32	7F	4D	
30	27	17	

31	68	59	Kolom ke-3
20	F2	D2	
4B	4D	06	
4D	17	5A	

45	59	1C	Kolom ke-4
44	D2	96	
41	06	47	
4E	5A	14	

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

48	68	59	1C
C2	F2	D2	96
7F	4D	06	47
27	17	5A	14

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:

48	68	59	1C
C2	F2	D2	96
7F	4D	06	47
27	17	5A	14

DA	B2	EB	F7
62	90	42	D4
85	C8	CE	89
BB	AC	F6	E2

....

35	11	F2	B2
A4	6A	D7	6B
D5	6D	94	8F
5B	2D	C2	27

2.3.2 Enkripsi

Proses enkripsi akan dilakukan pada *database* data administrasi anggota RAPI 0201 Kota Medan. *Plaintext* yang dienkripsi adalah "INDRA GUNAWAN", dengan proses enkripsi seperti berikut ini:

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

I	N	D	R	A		G	U	N	A	W	A	N			
49	4E	44	52	41	20	47	55	4E	41	57	41	4E	00	00	00

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

49	41	4E	4E
4E	20	41	00
44	47	57	00
52	55	41	00

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

49	41	4E	4E
4E	20	41	00
44	47	57	00
52	55	41	00

 \oplus

52	20	31	45
41	30	20	44
50	32	4B	41
49	30	4D	4E

 $=$

1B	61	7F	0B
0F	10	61	44
14	75	1C	41
1B	65	0C	4E

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*.

1B	61	7F	0B
0F	10	61	44
14	75	1C	41
1B	65	0C	4E

 \longrightarrow

AF	EF	D2	2B
76	CA	EF	1B
FA	9D	9C	83
AF	4D	FE	2F

- 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.

AF	EF	D2	2B
76	CA	EF	1B
FA	9D	9C	83
AF	4D	FE	2F

 \longrightarrow

AF	EF	D2	2B
CA	EF	1B	76
9C	83	FA	9D
2F	AF	4D	FE

- c. Selanjutnya adalah proses *MixColumns*, dimana proses ini akan melakukan perkalian antara dot product dengan *state* hasil dari *ShiftRows*.

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

 \times

AF	EF	D2	2B
CA	EF	1B	76
9C	83	FA	9D
2F	AF	4D	FE

Aturan dalam operator *polynomial* adalah jika dikali 01 maka hasilnya tetap, jika dikali 02 maka *bitshift* 1x ke kiri jika MSB = 0 dan *bitshift* 1x ke kiri diikuti operasi XOR dengan 11B (0001 0001 1011) jika MSB = 1, dan jika dikali 03 maka dilakukan operasi dikali 02 dan XOR dengan bilangan *hexadecimal* pada hasil bilangan *ShiftRows* itu sendiri. Berikut adalah uraian perkalian antara *polynomial* dengan hasil *ShiftRows*.

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

B3	C3	25	AF
B0	1B	BC	85
37	F7	F1	65
E2	03	16	71

 \oplus

48	68	59	1C
C2	F2	D2	96
7F	4D	06	47
27	17	5A	14

 $=$

FB	AB	7C	B3
72	E9	6E	13
48	BA	F7	22
C5	14	4C	65

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>			
0F	62	10	6D
40	1E	9F	7D
52	F4	68	93
A6	FA	29	4D

<i>ShiftRows</i>			
0F	62	10	6D
1E	9F	7D	40
68	93	52	F4
4D	A6	FA	29

<i>MixColumn</i>			
19	4B	0F	C7
C6	4F	E6	C3
16	31	DC	A5
FD	FD	F0	51

<i>RoundKey ke-2</i>			
DA	B2	EB	F7
62	90	42	D4
85	C8	CE	89
BB	AC	F6	E2

<i>AddRoundKey</i>			
C3	F9	E4	30
A4	DF	A4	17
93	F9	12	2C
46	51	06	B3

.....

Round ke-10

<i>SubBytes</i>			
D9	E7	30	6E
33	03	58	7A
D1	8F	32	B7
C4	FA	20	6A

<i>ShiftRows</i>			
D9	E7	30	6E
03	58	7A	33
32	B7	D1	8F
6A	C4	FA	20

<i>RoundKey ke-10</i>			
35	11	F2	B2
A4	6A	D7	6B
D5	6D	94	8F
5B	2D	C2	27

<i>AddRoundKey</i>			
EC	F6	C2	DC
A7	32	AD	58
E7	DA	45	00
31	E9	38	07

Hasil dari proses enkripsi yaitu: ECA7E731F632DAE9C2AD4538DC580007

2.3.3 Dekripsi

Proses ini dilakukan untuk mengembalikan data yang telah dienkripsi menjadi *plaintext* kembali. Transformasi deskripsi pada algoritma *advanced encryption standard* adalah *InvSubBytes*, *InvShiftRows*, *InvMixColumns*, dan *AddRoundKey*.

Berikut adalah proses dekripsi dari chipertext “ECA7E731F632DAE9C2AD4538DC580007”:

Melakukan proses XOR antara chipertext dengan *RoundKey* ke-10.

EC	F6	C2	DC
A7	32	AD	58
E7	DA	45	00
31	E9	38	07

 \oplus

35	11	F2	B2
A4	6A	D7	6B
D5	6D	94	8F
5B	2D	C2	27

 $=$

D9	E7	30	6E
03	58	7A	33
32	B7	D1	8F
6A	C4	FA	20

1. Selanjutnya, Pada *round* ke-1 sampai *round* ke-9 proses dekripsi dilakukan transformasi *InvShiftRows*, *InvSubBytes*, *InvMixColumns* dan *AddRoundKey*.

Round ke-1

InvShiftRows

D9	E7	30	6E
03	58	7A	33
32	B7	D1	8F
6A	C4	FA	20

D9	E7	30	6E
33	03	58	7A
D1	8F	32	B7
C4	FA	20	6A

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

D9	E7	30	6E
33	03	58	7A
D1	8F	32	B7
C4	FA	20	6A

 \longrightarrow

E5	B0	08	45
66	D5	5E	BD
51	73	A1	20
88	14	54	58

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

E5	B0	08	45
66	D5	5E	BD
51	73	A1	20
88	14	54	58

 \oplus

66	24	E3	40
0B	CE	BD	BC
0C	B8	F9	1B
52	76	EF	E5

 $=$

83	94	EB	05
6D	1B	E3	01
5D	CB	58	3B
DA	62	BB	BD

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

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

 \times

83	94	EB	05
6D	1B	E3	01
5D	CB	58	3B
DA	62	BB	BD

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</i> ke-8																																																
<table><tr><td>1D</td><td>FB</td><td>F3</td><td>0B</td></tr><tr><td>4D</td><td>EB</td><td>52</td><td>07</td></tr><tr><td>8D</td><td>2A</td><td>11</td><td>E8</td></tr><tr><td>67</td><td>92</td><td>EE</td><td>8E</td></tr></table>	1D	FB	F3	0B	4D	EB	52	07	8D	2A	11	E8	67	92	EE	8E	<table><tr><td>DE</td><td>63</td><td>7E</td><td>9E</td></tr><tr><td>65</td><td>3C</td><td>48</td><td>38</td></tr><tr><td>B4</td><td>95</td><td>E3</td><td>C8</td></tr><tr><td>0A</td><td>74</td><td>99</td><td>E6</td></tr></table>	DE	63	7E	9E	65	3C	48	38	B4	95	E3	C8	0A	74	99	E6	<table><tr><td>01</td><td>42</td><td>C7</td><td>A3</td></tr><tr><td>93</td><td>C5</td><td>73</td><td>01</td></tr><tr><td>6B</td><td>B4</td><td>41</td><td>E2</td></tr><tr><td>58</td><td>24</td><td>99</td><td>0A</td></tr></table>	01	42	C7	A3	93	C5	73	01	6B	B4	41	E2	58	24	99	0A
1D	FB	F3	0B																																															
4D	EB	52	07																																															
8D	2A	11	E8																																															
67	92	EE	8E																																															
DE	63	7E	9E																																															
65	3C	48	38																																															
B4	95	E3	C8																																															
0A	74	99	E6																																															
01	42	C7	A3																																															
93	C5	73	01																																															
6B	B4	41	E2																																															
58	24	99	0A																																															
<i>AddRoundKey</i>	<i>InvMixColumn</i>																																																	
<table><tr><td>DF</td><td>21</td><td>B9</td><td>3D</td></tr><tr><td>F6</td><td>F9</td><td>3B</td><td>39</td></tr><tr><td>DF</td><td>21</td><td>A2</td><td>2A</td></tr><tr><td>52</td><td>50</td><td>00</td><td>EC</td></tr></table>	DF	21	B9	3D	F6	F9	3B	39	DF	21	A2	2A	52	50	00	EC	<table><tr><td>7E</td><td>1C</td><td>F1</td><td>E1</td></tr><tr><td>F1</td><td>56</td><td>C5</td><td>EE</td></tr><tr><td>2D</td><td>55</td><td>AA</td><td>69</td></tr><tr><td>06</td><td>B6</td><td>BE</td><td>A4</td></tr></table>	7E	1C	F1	E1	F1	56	C5	EE	2D	55	AA	69	06	B6	BE	A4																	
DF	21	B9	3D																																															
F6	F9	3B	39																																															
DF	21	A2	2A																																															
52	50	00	EC																																															
7E	1C	F1	E1																																															
F1	56	C5	EE																																															
2D	55	AA	69																																															
06	B6	BE	A4																																															

.....

Round ke-10

<i>InvShiftRows</i>	<i>InvSubBytes</i>	<i>RoundKey</i> ke-0																																																
<table><tr><td>AF</td><td>EF</td><td>D2</td><td>2B</td></tr><tr><td>76</td><td>CA</td><td>EF</td><td>1B</td></tr><tr><td>FA</td><td>9D</td><td>9C</td><td>83</td></tr><tr><td>AF</td><td>4D</td><td>FE</td><td>2F</td></tr></table>	AF	EF	D2	2B	76	CA	EF	1B	FA	9D	9C	83	AF	4D	FE	2F	<table><tr><td>1B</td><td>61</td><td>7F</td><td>0B</td></tr><tr><td>0F</td><td>10</td><td>61</td><td>44</td></tr><tr><td>14</td><td>75</td><td>1C</td><td>41</td></tr><tr><td>1B</td><td>65</td><td>0C</td><td>4E</td></tr></table>	1B	61	7F	0B	0F	10	61	44	14	75	1C	41	1B	65	0C	4E	<table><tr><td>52</td><td>20</td><td>31</td><td>45</td></tr><tr><td>41</td><td>30</td><td>20</td><td>44</td></tr><tr><td>50</td><td>32</td><td>4B</td><td>41</td></tr><tr><td>49</td><td>30</td><td>4D</td><td>4E</td></tr></table>	52	20	31	45	41	30	20	44	50	32	4B	41	49	30	4D	4E
AF	EF	D2	2B																																															
76	CA	EF	1B																																															
FA	9D	9C	83																																															
AF	4D	FE	2F																																															
1B	61	7F	0B																																															
0F	10	61	44																																															
14	75	1C	41																																															
1B	65	0C	4E																																															
52	20	31	45																																															
41	30	20	44																																															
50	32	4B	41																																															
49	30	4D	4E																																															
<i>AddRoundKey</i>																																																		
<table><tr><td>49</td><td>41</td><td>4E</td><td>4E</td></tr><tr><td>4E</td><td>20</td><td>41</td><td>00</td></tr><tr><td>44</td><td>47</td><td>57</td><td>00</td></tr><tr><td>52</td><td>55</td><td>41</td><td>00</td></tr></table>	49	41	4E	4E	4E	20	41	00	44	47	57	00	52	55	41	00																																		
49	41	4E	4E																																															
4E	20	41	00																																															
44	47	57	00																																															
52	55	41	00																																															

Hasil dari proses dekripsi yaitu: 494E4452412047554E4157414E000000

3. ANALISA DAN HASIL

Merupakan kegiatan akhir dari proses penerapan sistem, dimana sistem ini akan dioperasikan secara menyeluruh. Sebelum sistem benar-benar bisa digunakan dengan baik, sistem harus melalui tahap pengujian analisa dan hasil terlebih dahulu untuk menjamin tidak ada kendala yang muncul pada saat sistem digunakan. Hasil dari penelitian yang dilakukan adalah sebagai berikut :

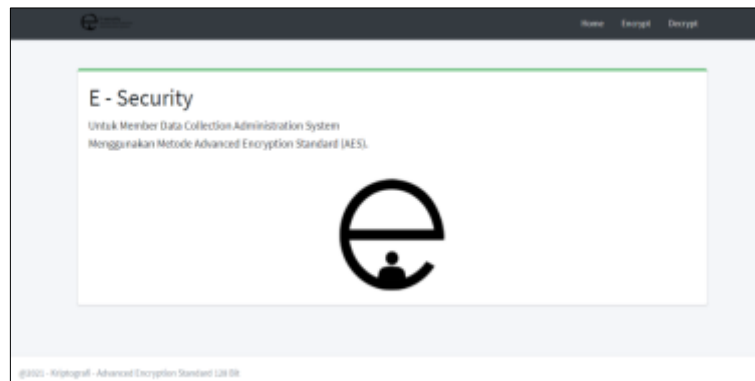
1. Struktur tabel *tbl_encrypt* dan *tbl_decrypt*
2. Berikut adalah struktur tabel *tbl_encrypt* dan *tbl_decrypt* yang digunakan dalam sistem sebagai berikut:

#	Nama	Jenis	Penyortiran	Atribut	Tak Termbil	Batasan	Komentar	Ekstra	Tindakan
<input type="checkbox"/>	1 id_anggota	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	2 nama	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	3 nomor_nik	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	4 tempat_lahir	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	5 tanggal_lahir	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	6 agama	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	7 jenis_kelamin	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	8 golongan_darah	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	9 alamat	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	10 kode_pos	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	11 no_hp	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	12 email	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	13 kontribusi_daerah	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	14 kontribusi_nasional	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	15 file_ktp	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya
<input type="checkbox"/>	16 katz_sandi	varchar(255)	utf8mb4_general_ci	Ya	NULL				Ubah Hapus Lainnya

Gambar 3.1 Struktur tabel tbl_encrypt dan tbl_decrypt

3.1 Tampilan Menu Utama (Home)

Berikut adalah menu utama (*home*) dari *website* yang dirancang sebagai halaman paling awal dari sistem yaitu:



Gambar 3.2 Tampilan Menu Utama (Home)

3.2 Tampilan Halaman Menu *Encrypt* dan *Decrypt*

Berikut adalah halaman *Encrypt* untuk melakukan enkripsi terhadap *database* data anggota RAPI 0201 Kota Medan yaitu:

Gambar 3.3 Tampilan Menu *Encrypt* dan *Decrypt*

3.3 Tampilan Hasil *Encrypt*

Berikut adalah hasil *Encrypt* pada saat proses enkripsi terhadap *database* data anggota RAPI 0201 Kota Medan berhasil dilakukan yaitu:

id_anggota	nama	nomor_nik	tempat_lahir	tanggal_lahir	agama
IAJWYV+8v2	IQWwF+8v2AuRlUeEgjeWRQhqcq	lgZNI+8v2CZ2xKaZAheEtIECv3Ruf6	lwK36i+8v2BvYS+JHG	lwKwDi+8v2DaZyF5RWBip0	mALU+8v2DabDriHig==
CAP9i+8v2C	DAPGai+8v2BwRDlp3v9fKCCzqNhzvD0Xa	EQ0M6i+8v2AF9iV5ndw8v8dmeBzE	FAP9ai+8v2CiaDLBA:	FuMwF+8v2A67D543n1ufPG	GpP4yH+8v2C0G6wv9g==
uQOFCV+8v	agNjH+8v2CFLGvYSP	aaOCn+8v2C4LXSvWgg9ZyFOKZ4sd	baOgh+8v2Btw7w4Q	lQNMV+8v2CRlulj24y0mD	bwP5emV+8v2AYghKpK==
ZAMid+8v2	ZAMyH+8v2ACVYC4eNO3ZyXlglr1WQ91Hh	ZQOK9F+8v2B0XF9CZ91QMTB0X2b3c	ZQMCRV+8v2Cv7Su2w	ZQOm8F+8v2A+slgGouRVWV9s	ZgPp+1+8v2BQZECdHe==
HgCk2C8vZl	HeAse2C8vZDFZVmbRSEB73TPq	HeD6TGC8v2C8Vp3nnkAQZMFGMkx8d	HeA3TmC8v2DkR9Gt	IAB6UWC8v2AS4Q+WNHvCA7	IAP92C8v2BKw7m9w=

Gambar 3.5 Tampilan Hasil *Encrypt*

3.5 Tampilan Hasil *Decrypt*

Berikut adalah hasil *Decrypt* pada saat proses enkripsi terhadap *database* data anggota RAPI 0201 Kota Medan berhasil dilakukan yaitu:

id_anggota	nama	nomor_nik	tempat_lahir	tanggal_lahir	agama
1	Indra Gunawan	1271112010710006	P. Siantar	1971-10-20	Islam
2	Dudi Rahmadiansyah	1271212108780001	Bunut	1978-08-21	Islam
3	Julani	1271115707650000	Medan	1969-07-17	Islam
4	Sughartono S Sos M Si	1271130703620000	Medan	1962-03-07	Islam
5	Hanafi Maksum	1207261066740010	Medan	1974-06-18	Islam

Gambar 3.6 Tampilan Hasil *Decrypt*

4. KESIMPULAN

Berdasarkan masalah yang telah dipaparkan pada pembahasan sebelumnya maka dapat ditarik kesimpulan bahwa dibangunnya sistem pengamanan *database* anggota organisasi RAPI 0201 Kota Medan, algoritma *advanced encryption standard* 128 bit berhasil diterapkan.

Dalam penerapan sistem *E-Security* berbasis *web* mengenai keamanan *database* organisasi RAPI 0201 Kota Medan khususnya terkait data anggota dapat digunakan dan kebutuhan pada sistem telah sesuai dengan kebutuhan dalam pengamanan *database* anggota RAPI 0201 Kota Medan.

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 Azanuddin,S.Kom.,M.Kom selaku Dosen Pembimbing I, kepada Ibu Ita Mariami,S.E.,M.Si selaku Dosen Pembimbing II yang telah banyak membantu dalam memberikan arahan dan bimbingan.

REFERENSI

[1] W. Wihayati, “Analisis Komunikasi Kesehatan Dalam Pengelolaan Sampah Bekas Pakai Di Desa Pegagan Kecamatan Palimanan Kabupaten Cirebon,” vol. 8, no. 2, 2020.




[2] R. Firmansyah and A. A. Permana, “Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma RSA dengan Metode Waterfall Berbasis Java,” vol. 4, no. 1, pp. 217–221, 2019.

[3] A. Y. Mulyadi, E. P. Nugroho, and R. R. J. P, “Implementasi Algoritma AES 128 dan SHA – 256 Dalam Pengkodean pada Sebagian Frame Video CCTV MPEG-2,” *JATIKOM J. Teor. dan Apl. Ilmu Komput.*, vol. 1, no. 1, pp. 33–39, 2018.

[4] D. Novianto and Y. Setiawan, “Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES),” *J. Ilm.*

- Inform. Glob.*, vol. 9, no. 2, pp. 83–89, 2019, doi: 10.36982/jig.v9i2.561.
- [5] Asiyanik, “Studi Terhadap Advanced Encryption Standard (Aes) Dan Algoritma Knapsack Dalam Pengamanan Data,” *Santika*, vol. 7, no. Jurnal Ilmiah Sains dan Teknologi, pp. 553–561, 2017.
- [6] K. Zalukhu, Y. Syahra, and T. Syahputra, “Implementasi Sistem Keamanan Database Data Menggunakan Algoritma Advanced Encryption Standard 128 Bit pada Pengadilan Militer I-02 Medan,” vol. 3, no. 2, pp. 138–150, 2020.
- [7] D. Ariyus, “Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi,” *Journal of Chemical Information and Modeling*. 2008.

BIBLIOGRAFI PENULIS

	<p>Nama : Lutfita Andini Tempat/Tgl : Medan, 16 April 2001 Alamat : Jl. Eka Suka VIII No. 2 Kel. Gedung Johor Agama : Islam Jenis Kelamin : Perempuan No.Hp : 0813-9659-4365 Bidang Keilmuan : Kriptografi dan Desain Grafis E-mail : lintangkasa@gmail.com</p>
	<p>Nama : Azanuddin, S.Kom., M.Kom Tempat/Tgl : Klambir Lima, 26 Juni 1989 Alamat : Dusun XI Gg. Mardisan Agama : Islam Jenis Kelamin : Laki-Laki N0.Hp : 0813-7683-7222 Prestasi Dosen : - Bidang Keilmuan : Jaringan, Mobile, dan Sistem Terdistribusi Email : azdin.bpc@gmail.com</p>
	<p>Nama : Ita Mariami, SE., M.Si Tempat/Tgl : Mambang Muda, 03 April 1966 Alamat : Jl. Eka Bakti Komp. Griya No. A4 Medan Agama : Islam Jenis Kelamin : Perempuan N0.Hp : 0813-7041-7023 Prestasi Dosen : Dosen Terbaik STMIK TRIGUNA DHARMA TAHUN 2018 Bidang Keilmuan : E-Bisnis Dan Manajemen Email : itamariami66@gmail.com</p>