Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

Implementasi Kriptografi Untuk Pengamanan Data Aset Perusahaan Pada PT.PLN (Persero) Dengan Menggunakan Metode Algoritma AES 192

Nazmi May Sarah Sianturi[*], Nurcahyo Budi Nugroho[**], Widiarti Rista Maya[**]
[*] Program Studi Sistem Informasi, STMIK Triguna Dharma
[**] Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info
Article history:

Keyword:
Kriptografi, Advanced Encryption Standard, PLN

ABSTRACT

PT. PLN (Persero) P3BS UPT MEDAN adalah PT PLN (Persero) Penyaluran dan Pengatur Beban Sumatera (P3B Sumatera). P3B Sumatera bukanlah lembaga yang benar-benar baru. Sebab P3B Sumatera merupakan penggabungan fungsi penyaluran dari PT PLN (Persero) Kitlur Sumbagut dan fungsi penyaluran PT PLN (Persero) Kitlur Sumbagut.

Keamanan data adalah sesuatu yang sangat penting untuk melindungi kerahasiaan informasi kumpulan data yang sangat penting. Diperlukan suatu teknik pengamanan tambahan untuk menjaga suatu keamanan informasi penting tersebut. sebelum adanya teknik tambahan untuk menjaga suatu kerahasiaan data, bakalan banyak terjadi melakukan hal yang tidak diinginkan yaitu serangan yang tidak bertanggung jawab, salah satunya adalah pencurian data. menggunakan algoritma kriptografi suatu cara yang tepat untuk melindungi kerahasiaan informasi data.

Dari penelitian yang akan dibahas ini diharapkan sistem yang akan dirancang nanti akan membantu pihak perusahaan atau bagian staff yang memegang kendali bagian data aset perusahaan.

First Author
Nama : Nazmi May Sarah Sianturi
Program Studi : Sistem Informasi STMIK Triguna Dharma
Email : sarahnazmi22@gmail.com

1. PENDAHULUAN

PT. PLN (Persero) P3BS UPT MEDAN adalah PT PLN (Persero) Penyaluran dan Pengatur Beban Sumatera (P3B Sumatera). P3B Sumatera bukanlah lembaga yang benar-benar baru. Sebab P3B Sumatera merupakan penggabungan fungsi penyaluran dari PT PLN (Persero) Kitlur Sumbagut dan fungsi penyaluran PT PLN (Persero) Kitlur Sumbagut.

Meskipun demikian, sebagai penyelenggara transaksi energi P3B Sumatera wajib memberikan pasokan listrik secara handal, ekonomis dan berkualitas kepada konsumennya. Seperti yang usdah dibahas PT. PLN (Persero) P3BS UPT Medan sendiri adalah salah satu anak perusahaan BUMN yang cukup besar, dengan begitu banyak data-data yang sangat rahasia yang sangat di jaga oleh perusahaan agar tidak bocor dan disalah gunakan oleh orang-orang yang tidak bertanggung jawab, salah satunya adalah data aset perusahaan PT. PLN (Persero) P3BS UPT Medan.

Keamanan data adalah sesuatu yang sangat penting untuk melindungi kerahasiaan informasi kumpulan data yang sangat penting. Diperlukan suatu teknik pengamanan tambahan untuk menjaga suatu keamanan informasi penting tersebut. sebelum adanya teknik tambahan untuk menjaga suatu kerahasiaan data, bakalan banyak terjadi melakukan hal yang tidak diinginkan yaitu serangan yang tidak bertanggung jawab, salah satunya adalah pencurian data. menggunakan algoritma kriptografi suatu cara yang tepat untuk melindungi kerahasiaan informasi data.

Dari penelitian yang akan dibahas ini diharapkan sistem yang akan dirancang nanti akan membantu pihak perusahaan atau bagian staff yang memegang kendali bagian data aset perusahaan.

Berdasarkan masalah yang dihadapi, maka penulis mengangkat judul sebagai inti pembahasan dalam penelitian yaitu **"*Implementasi Kriptografi Untuk Pengamanan Data Aset Perusahaan Pada PT.PLN (Persero) Dengan Menggunakan Metode Algoritma AES 192*"**

2. KAJIAN PUSTAKA

2.1 Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi. Contoh algoritma kriptografi yang dapat dihandalkan adalah RSA, dimana RSA merupakan proses penyandian kunci asimetrik (*asymmetric key*). Proses perumusan RSA didasarkan pada *Teorema Euler*, sedemikian sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitan [5].

2.2 Advanced Encryption Standard

AES merupakan algoritma kriptografi bernama Rijndael yang dirancang oleh dua orang kriptografer yang berasal dari Belgia yaitu Vincent Rijmen dan John Daemen. Mereka merupakan pemenang kontes algoritma kriptografi pengganti *Data Encryption Standard* (DES) yang diadakan oleh *National Institutes of Standards and Technology* (NIST) di Amerika Serikat pada tanggal 26 November 2001.

AES *(Advanced Encryption Standard)* dibuat untuk menggantikan standar enkripsi kriptografi yang lama dimana sudahh tidak terjamin lagi keamanannya yaitu DES *(Data Encryption Standard).* Algoritma AES disebut algoritma dengan *cipher block symmetric* karena untuk memperoleh data yang telah dienkripsi menggunakan kunci rahasia yang sama ketika melakukan proses penyandian data.

2.3 Algoritma Advanced Encryption Standard

1. *Key Schedule*

Key Schedule berfungsi untuk menentukan hasil *subkey* dari kunci utama untuk melakukan proses enkripsi dan dekripsi. Operasi ini terdiri dari :

   a. *Rotate*, merupakan proses perputaran kunci 8-bit menjadi 32-bit.
   b. *SubByte*, merupakan proses substitusi dari 8-bit *subkey* dengan nilai dari tabel *S-box*.
   c. *Rcon*, operasi ini menggunakan nilai dalam *galois field* kemudian di XORkan dengan hasil operasi *subbytes* sesuai dengan nilai yang diinginkan *user* yang dipangkatkan 2.
   d. Operasi pada XOR dengan w[i-Nk] yaitu *word* yang berada pada Nk sebelumnya.

2. *Addroundkey*

Pada tahap ini dilakukan kombinasi *chipertext* yang sudah ada dengan *chiperkey* yang dihubungkan dengan XOR.

3. *SubByte*

SubByte ialah transformasi *byte* dimana pada setiap elemen *state* akan dipetakan menggunakan sebuah tabel substitusi *(S-Box).*

4. *Shiftrows*

Pada tahap ini dilakukan pergeseran tiap baris dari tabel *state*. Pada baris pertama tidak dilakukan pergeseran, pada baris kedua dilakukan pergeseran 1-*byte*, pada baris ketiga dilakukan pergeseran 2-*byte* dan pada baris keempat dilakukan pergeseran 3-*byte.*

5. *MixColumns*

Proses ini dilakukan perkalian tiap elemen dari *block chipper* dengan matriks. Pengalian dilakukan seperti perkalian biasa menggunakan *dot*
product kemudian perkalian keduanya dimasukkan ke dalam sebuah *block chipper* baru. Persamaan *mixcolumns* dapat dilihat pada gambar dibawah ini.

waktu yang dibutuhkan tergantung dariamasing-masing data yang akan didekripsi. Beberapa data membutuhkan waktu yang relatif lebihasingkat dari proses enkripsi, ada beberapaayang membutuhkan tambahan waktu lebih lamaasepersekian detik.

3. METODOLOGI PENELITIAN

Untuk mempermudah penelitian ini dalam penentuan metodologi adalah hal terpenting, karena metode penelitian merupakan prosedur atau langkah-langkah dalam mendapatkan pengetahuan yang digunakan seseorang dalam melakukan kegiatan penelitian, jadi metode penelitian merupakan cara sistematis untuk menyusun ilmu pengetahuan dalam memecahkan masalah penelitian dan dapat dipahami sebagai ilmu yang mempelajari bagaimana penelitian dilakukan secara ilmiah.

Didalam metode penelitian ini terdapat beberapa langkah yaitu *data collecting* atau pengumpulan data dan *studi literatur.* Penjelasannya adalah sebagai berikut:

1. *Data Collecting*

Dalam teknik pengumpulan data terdapat beberapa hal yang harus dilakukan di antaranya yaitu sebagai berikut:

a. Observasi

Observasi merupakan teknik pengumpulan data, metode ini dipakai untuk mengumpulkan keterangan atau data dengan cara mengamati dan mencatat fenomena-fenomena yang terjadi pada sasaran pengamatan.

b. Wawancara

Wawancara merupakan metode pengumpulan data, dilakukan dengan cara interaksi dengan komunikasi interpersonal yang melibatkan dua orang atau lebih dalam sebuah percakapan yang berbentuk tanya jawab.

2. *Studi Literatur*

Dalam *studi literartur*, tahap ini dilakukan cara pengumpulan data mengunakan jurnal-jurnal baik jurnal internasional, jurnal nasional, jurnal lokal maupun buku sebagai sumber referensi.

3.1 Metode Perancangan Sistem

Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode *waterfall*. Metode *waterfall* merupakan model pengembang sistem informasi yang menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau terurut dimulai dari analisis, desain, pengodean, pengujian, dan tahap pendukung (*support*). Berikut ini adalah fase yang dilakukan dalam penelitian ini yaitu:

1. Analisis Kebutuhan Perangkat Lunak.
2. Desain.
3. Pembuat Kode Program.
4. Pengujian.
5. Pendukung (*support*) atau pemeliharaan (*maintenance*).

3.2 Algoritma Sistem

Pada pengembangan penulis mengunakan metode Air terjun (*WaterFall*) Menurut Rosa dan M. Shalahuddin (2013:28) Model SDLC air terjun (*waterfall*) sering juga disebut model sekuensial linier (*sequential linier*) atau alur hidup klasik (*classic life cycle*). Model air terjun menyediakan pendekatan alur hidup perangkat lunak secara sekuential atau terurut dimulai dari analisis, desain, pengkodean, pengujian, dan tahap pendukung (*support*).

1. Analisis Kebutuhan Perangkat Lunak

Proses pengumpulan kebutuhan dilakukan secara intensif untuk menspesifikasikan kebutuhan perangkat lunak agar dapat dipahami perangkat lunak seperti apa yang dibutuhkan oleh user. Spesifikasi kebutuhan perangkat lunak pada tahap ini perlu untuk didokumentasikan.

2. Desain

Desain perangkat lunak adalah proses multi langkah yang fokus pada desain pembuatan program perangkat lunak termasuk struktur data, arsitektur perangkat lunak, representasi antarmuka, dan prosedur pengkodean. Tahap ini mentrannslasi kebutuhan perangkat lunak dari tahap analisis kebutuhan ke representasi desain agar dapat diimplementasikan menjadi program pada tahap selanjutnya. Desain perangkat lunak yang dihasilkan pada tahap ini juga perlu didokumentasikan.

   a. Pembuatan Kode Program Desain
      harus ditranslasikan kedalam program perangkat lunak. Hasil dari tahap ini adalah program komputer sesuai dengan desain yang telah dibuat pada tahap desain.
   b. Pengujian
      Pengujian fokus pada perangkat lunak secara dari segi lojik dan fungsional dan memastikan bahwa semua bagian sudah diuji. Hal ini dilakukan untuk meminimalisir kesalahan (*error*) dan memastika keluaran yang dihasilkan sesuai dengan yang diinginkan.

3. Pendukung atau Pemeliharaan (*maintenance*)

Tidak menutup kemungkinan sebuah perangkat lunak mengalami perubahan ketika sudah dikirimkan ke user. Perubahan bisa terjadi karena adanya kesalahan yang muncul dan tidak terdeteksi saat pengujian atau perangkat lunak harus beradaptasi dengan lingkungan baru. Tahap pendukung atau pemeliharaan dapat mengulangi proses pengembangan mulai dari analisis spesifikasi untuk perubahan perangkat lunak yang sudah ada, tapi tidak untuk membuat perangkat lunak baru.

3.2.1 Penyelesaian

Berikut ini adalah data *aset* yang didapat dari PT.PLN Medan, yang akan diamankan. Dalam pengujiannya, sebagai contoh data yang digunakan sebagai sampel dalam penelitian ini yaitu sebagai berikut:

Tabel 3.2 Sampel Data *Aset* di PT.PLN Medan

NO	Company Code	Asset No	Nama Aset	Harga	Spesifikasi
1	3200	1000026965	NGR (NEUTRAL GROUNDING RESISTENCE)	Rp. 261.834.508	merk RESISTEL, type 1 frame
2	3200	1000027115	BUSBAR	Rp. 44.819.432	type AAC 1000
3	3200	1000131570	PANEL CONTROL	Rp. 184.590.969	Type AAB
4	3200	1000136752	RELAY OCR	Rp. 20.525.381	merk THOSIBA, type TCO23B
5	3200	1000028513	TRAFO POWER	Rp. 1.915.483.571	merk PAUWELS, type ORF.60/275
6	3200	1000236752	GENSET	Rp. 139.307.971	-
7	3200	1000130828	GANTRY	Rp. 409.568.555	-
8	3200	1000130612	LIGHTNING ARRESTER (LA)	Rp. 100.893.991	type SB 150/20.4-1, TRIDELTA
9	3200	1000130083	CIRCUIT BREAKER (CB)	Rp. 230.998.081	type SB.72,merk NOUVA MAGRINI GALILE
10	3200	1000130310	DISCONNECTING SWITCH (DS)	Rp. 129.594.849	type S2DAT,merk COELME

3.3.3 Penyelesaian Masalah Dengan Algoritma

Sesuai dengan referensi yang telah dipaparkan pada bab sebelumnya, berikut ini adalah langkah-langkah penyelesaiannya yaitu:

3.3.3.1 Proses Enkripsi AES

Proses enkripsi algoritma AES, ada dua tahapan yaitu proses ekspansi kunci dan proses enkripsi.

1. Proses Ekspansi Kunci

Kunci ronde (*round key*) dibutuhkan untuk proses enkripsi dan dekripsi pada algoritma *Advanced Encryption Standart*. Maksimal panjang kunci adalah 16 digit dan jumlah kunci ronde nya adalah 10 kunci ronde yang diperoleh dari proses ekspansi kunci. Pada kasus ini, kunci yang akan digunakan yaitu: "datapenjualanobt".

a. Urutkan kunci kedalam blok berukuran 192 bit (24 kode ASCII). Lalu ubah kunci kedalam bentuk heksadecimal

N	A	Z	M	I		M	A	Y		S	A	R	A	H		S	I	A	N	T	U	R	I
4E	41	5A	4D	49	20	4D	41	59	20	53	41	52	41	48	20	53	49	41	4E	54	55	52	49

b. angkah selanjutnya yaitu susun kunci yang telah diubah kedalam bentuk heksadesimal kedalam state berukuran 4 × 6 seperti dibawah ini :

4E	49	59	52	53	54
41	20	20	41	49	55
5A	4D	53	48	41	52
4D	41	41	20	4E	49

State diatas merupakan *chiperkey*/kunci *rounde* ke-0

c. Setelah itu, untuk mendapatkan kolom pertama pada sub kunci, langkah pertama yaitu dilakukan fungsi *RotWord*, yaitu dengan menggeser setiap bit pada kolom ke-4 ke atas 1 kali dari kunci ronde ke-0.
d. Kemudian hasil dari *RotWord* tersebut disubtitusikan dengan nilai pada tabel *S-Box* (*SubBytes*).
e. Tahap yang terakhir yaitu lakukan proses *XOR* antara kolom pertama dari kunci *ronde* ke-0, hasil dari *SubBytes* lalu di-*XOR*-kan lagi dengan *RCon*. Kolom pertama (wi) pada kunci ronde selanjutnya (ronde ke-1) = K1
f. Untuk mendapatkan kolom kedua, diperoleh dari proses *XOR* antara Wi dengan kolom kedua dari kunci ronde ke-0. Sedangkan untuk mendapatkan kolom ketiga dan keempat kunci ronde ke-1, dilakukan proses seperti memperoleh kolom kedua.

Kolom ke-2

B3		49		FA				
41	⊕	20	=	61				
61		4D		2C				
6D		41		2C				

Kolom ke-3

FA		59		A3				
61	⊕	20	=	41				
2C		53		7F				
2C		41		6D				

Kolom ke-4

A3		52		F1				
41	⊕	41	=	00				
7F		48		37				
6D		20		4D				

F1		53		A2				
00	⊕	49	=	49				
37		41		76				
4D		4E		03				

A2		54		F6				
49	⊕	55	=	1C				
76		52		24				
03		49		4A				

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

g. seluruh proses diatas, maka telah didapatlah ekspansi kunci untuk ronde ke-1 yaitu :

B3	FA	A3	F1	A2	F6
41	61	41	00	49	1C
61	2C	7F	37	76	24
6D	2C	6D	4D	03	4A

Untuk mendapatkan kunci ronde ke-2 sampai ke-10, proses diatas diulang 10 kali. Dibawah ini adalah hasil ekpansi kunci dari ronde ke 1 sampai ronde 10:

RoundKey Ke-1

53	54	B3	FA
49	55	41	61
41	52	61	2C
4E	49	6D	2C

RoundKey Ke-2

A3	F1	A2	F6
41	00	49	1C
7F	37	76	24
6D	4D	03	4A

RoundKey Ke-3

2D	D7	74	85
77	16	57	57
B7	9B	E4	D3
2F	03	6E	23

RoundKey Ke-4

27	D1	5E	89
1E	02	7B	6D
A5	81	B5	2E
20	6A	11	12

RoundKey Ke-5

FD	78	5F	8E
3A	6D	73	71
CA	19	BC	3D
7C	5F	7F	15

RoundKey Ke-6

F5	7C	81	F9
5C	31	0B	66
EC	C2	08	11
08	1A	66	39

RoundKey Ke-7

A6	28	A6	DA
15	64	3C	0D
AD	90	01	C3
46	53	3C	26

RoundKey Ke-8

5B	A2	04	2C
06	60	75	11
CB	DA	77	E7
40	79	3F	6C

RoundKey Ke-9

04	DE	85	27
A8	A5	A3	C3
51	92	59	83
4D	6B	2B	52

RoundKey Ke-10

23	0F	18	C6
B6	A7	D5	70
F4	13	2D	BF
6D	01	3B	50

RoundKey Ke-11

43	64	47	48
D3	10	A6	01
E6	65	91	82
7B	29	44	45

RoundKey Ke-12

E4	22	61	05
C6	B6	65	75
43	FC	1A	7F
69	39	42	6B

2. Proses Enkripsi

Plaintext yang akan digunakan adalah" PT. PLN (Persero) P3BS UPT Medan"

T	R	A	F	O	P	W	R		P	A	U	W	E	L	S
54	52	41	46	4F	50	57	52	20	50	41	55	57	45	46	53

Susun 16 *byte* pertama dari *plaintext* yang telah diubah kedalam *state* 4x4:

54	4F	20	57
52	50	50	45
41	57	41	4C
46	52	55	53

Lakukan *XOR* antara *plaintext* dengan *roundKey* 0. Proses ini dinamakan *AddRoundKey*.

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

54	4F	20	57
52	50	50	45
41	57	41	4C
46	52	55	53

⊕

4E	49	59	52
41	20	20	41
5A	4D	53	48
4D	41	41	20

=

1A	06	79	05
13	70	70	04
1B	1A	12	04
0B	13	14	73

Proses *AddRoundkey* diatas masih sebagai *Pra-rounde* dan akan menjadi masukan untuk *rounde* ke-1 yang akan di proses dengan 4 transformasi yaitu: *SubBytes*,*Shiftrows*,*MixColumns*,dan *AddRoundeKey*.

1. Hasil dari *Pra-Rounde* disubtitusikan dengan nilai pada table *S-Box(SubBytes*).

2. Lakukan *Shiftrows* pada hasil subtitusi *SubBytes* yang dieksekusi lewat pergeseran *siklik* secara memutar dengan geseran yang acak pada tiga baris terakhir *state* (baris pertama r = 0,tidak digeser). Baris ke dua digeser secara siklik ke kiri sekali,baris ke tiga dua kali, dan baris ke empat tiga kali.
3. Transformasi *MixColumns* dengan mengoperasikan *state* kolom demi kolom pada *state* kolom, dengan mengkonversikan setiap kolom dengan *polynomial*.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

$b0.a_0 = (A2).(02)$

$= (10100010) .(10)$

$= (x^7+x^5+x). (x)$

$= x^8+x^6+x^2$

$=(x^4+x^3+x+1)+x^6+ x^2$

$=x^6+x^4+x^3+ x^2+x+1$

$=01011111$

$=5F$

$a_1 = (51) .(03)$

$= (01010001) . (11)$

$= (x^6+x^4+x+1) . (x+1)$

$= x^7+x^6+x^5+ x^4 x+1$

$=11110011$

$= F3$

$a_2 = (C9) . (1) = 11001001$

$a3 = (8F) . (1) = 10001111$

01011111 x 11110011 x 11001001 x 10001111 = EA

10100010 x 10100010 x 01000000 x 10001111 = CF

10100010 x 01010001 x 10001001 x 10001010 = FO

11111101 x 01010001 x 11001001 x 00000101 = 60

Lakukan perulangan seperti yang diatas,sehingga di dapatkan hasil *MixColumns* seperti sebagai berikut.

4. Langkah terakhir untuk mendapatkan enkripsi putaran pertama,lakukan *XOR* antara hasil *MixColumns* dengan *RoundKey* ke-1, proses ini disebut *AddRoundKey*.

MixColumns					*Roundekey* ke-1					*AddRoundeKey*			
EA	F4	A8	09	⊕	53	54	B3	FA	=	B9	A0	1B	F3
CF	EB	DE	96		49	55	41	61		86	BE	9F	F7
F0	BC	86	5C		41	52	61	2C		B1	EE	E7	70
60	44	66	8D		4E	49	6D	2C		2E	0D	0B	A1

Hasil dari proses *AddRoundKey* atau *rounde* ke-10 di ubah ke bentuk karakter didalam table ASCII.

Tabel 3.4 *rounde* kode ASCII untuk *Ciphertext*

Rounde	ASCII	Karakter
EB	235	ë
4A	74	J
5E	94	^
19	25	
D6	214	Ö
67	103	g
1B	27	ESC
50	80	P
E1	225	Ÿ
D3	211	Ó
28	40	(
CE	206	Î
C6	198	Æ
A1	161	¡
4A	74	J
B7	183	·

Dan hasil dari enkripsi dengan algoritma AES menghasilkan Ciphertext sebagai berikut:
235,74,94,25,214,103,27,80,225,211,40,206,198,161,74,183

3.3.3.2 Proses Dekripsi Algoritma AES

Kunci yang digunakan untuk proses dekripsi sama dengan yang digunakan pada proses enkripsi. Berikut adalah proses dekripsi dari hasil *ciphertext* yang telah diperoleh dari proses enkripsi sebelumnya.

EB	4A	5E	19	D6	67	1B	50	E1	D3	28	CE	C6	A1	4A	B7

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

Kemudian susun 16 byte pertama dari *ciphertext* yang telah diubah ke bentuk hexadesimal ke dalam *state* 4x4:
Lakukan *XOR* antara *Ciphertext* dengan *RoundKey* 12. Proses ini dinamakan *AddInvRoundKey*.

EB	D6	E1	C6	⊕	E4	22	61	05	=	0F	F4	80	C3
4A	67	D3	A1		C6	B6	65	75		8C	D1	B6	D4
5E	1B	28	4A		43	FC	1A	7F		1D	E7	32	35
19	50	CE	B7		69	39	42	6B		70	69	8C	DC

Proses *AddInvRoundkey* diatas masih sebagai *Initial-rounde* dan akan menjadi masukan untuk *rounde* ke-1 yang akan di proses dengan 4 transformasi yaitu: *InvShiftrows,InvSubBytes*, *AddInvRoundKey* dan *InvMixColumns*,

a. Lakukan *InvShiftrows* pada hasil *Initial-Rounde* yang dieksekusi lewat pergeseran siklik ecara memutar. Baris ke dua digeser secara siklik ke kiri tiga kali, baris ke tiga dua kali, baris ke empat sekali.
b. Hasil dari *InvShiftrows* disubtitusikan dengan nilai pada tabel *S-Box*$^{-1}$ *(InvSubBytes).*
c. XOR hasil dari *InvSubBytes* dengan *RoundKey* ke-11. Proses ini disebut *AddInvRoundKey*.

FB	BA	3A	33	⊕	43	64	47	48	=	B8	DE	7D	7B
19	F0	51	79		D3	10	A6	01		CA	E0	F7	78
A1	D9	DE	B0		E6	65	91	82		47	BC	4F	32
E4	F0	93	D0		7B	29	44	45		9F	D9	D7	95

d. Hasil dari *AddInvRoundKey* ditransformaikan oleh *InvMixColumns* dengan mengoperasikan *state* kolom demi kolom. Operasi ini di lakukan pada *state* kolom,dengan mengkonversikan setiap kolom sebagai *polynomial*.

Lakukan perulanagan seperti yang di atas,hingga didapatkan hasil InvMixColumns seperti sebagai berikut.

Proses diatas diulang sampai 12 kali putaran (*round*). Berikut adalah hasil dari dekripsi hingga *round* ke-12.

Rounde ke-1

B8	DE	7D	7B
CA	E0	F7	78
47	BC	4F	32
9F	D9	D7	95

Rounde ke-2

71	40	6E	90
6A	E7	95	AF
37	1D	D1	D3
B1	36	4D	D2

Rounde ke-3

89	CA	CC	65
1B	32	43	57
0D	10	FB	9E
2B	43	93	4C

Rounde ke-4

25	02	CA	F4
84	87	8F	8E
2F	22	47	E5
A3	E5	96	61

Rounde ke-5

05	0E	E5	44
C9	FA	47	7B
B0	B1	47	93
77	6A	DA	29

Rounde ke-6

47	7F	AC	36
C8	F4	B2	83
DC	9F	EF	26
EA	B8	BE	EE

Rounde ke-7

14	F4	83	7A

Rounde ke-8

88	88	1B	4C

Rounde ke-9

68	57	1D	59

3D	28	4D	2A
9D	F4	3F	0C
B1	51	37	D7

Rounde ke-10

4C	67	B3	BB
CD	48	A1	75
20	2E	06	4B

Rounde ke-11

D4	59	59	3D
3A	BF	4B	E3
13	B4	E1	E3

Rounde ke-12

E3	CD	E2	D5
84	8F	EB	D6
9D	CA	2E	64
A4	D3	FF	2D

EA	F4	A8	09
CF	EB	DE	96
F0	BC	86	5C
60	44	66	8D

A2	6F	B6	6B
51	51	F2	7D
C9	F2	AF	A2
8F	2B	7D	FA

Khusus round ke-10 transformasi *InvMixColumns* tidak dilakukan, cukup hanya transformasi *InvShiftrows*, *InvSubBytes*, dan *AddInvRoundKey*.

1. InvShiftrows

A2	6F	B6	6B
51	51	F2	7D
C9	F2	AF	A2
8F	2B	7D	FA

2. InvSubBytes

A2	6F	B6	6B
7D	51	51	F2
AF	A2	C9	F2
2B	7D	FA	8F

3. AddInvRoundKey

1A	06	79	05
13	70	70	04
1B	1A	12	04
0B	13	14	73

$\oplus$

4E	49	59	52
41	20	20	41
5A	4D	53	48
4D	41	41	20

=

54	4F	20	57
52	50	50	45
41	57	41	4C
46	52	55	53

Hasil dari proses *AddRoundKey* atau *Round* ke-10 ubah ke bentuk karakter di dalam tabel ASCII.

Tabel 3.5 *rounde* kode ASCII dan karakter untuk *Plaintext*

Rounde	Kode ASCII	Karakter
70	112	P
74	116	T
2E	46	.
6D	109	M
65	101	E
73	115	S

74	116	T
69	105	I
6B	107	K
61	97	A
20	32	SPASI
73	115	S
61	97	A
6B	107	K
74	116	T
69	105	I

Dan hasil dari dekripsi dengan algoritma AES menghasilkan *Plaintext*.
112, 116, 46, 109, 101, 115, 116, 105, 107, 97, 32, 115, 97, 107, 116, 105

4. PEMODELAN SISTEM DAN PERANCANGAN

Pemodelan merupakan suatu rencana atau rancangan yang menjelaskan mengenai suatu objek yang akan dibuat. Sedangkan sistem adalah suatu jaringan kerja yang saling berhubungan satu dengan yang lainnya dalam melakukan kegiatan untuk mencapai suatu tujuan. Dari kedua defenisi tersebut dapat disimpulkan bahwa pemodelan sistem merupakan suatu rancangan dalam membangun objek atau pola dari suatu sistem secara menyeluruh agar memudahkan pemahaman dari informasi yang dibutuhkan.

Berikut ini adalah penjelasan mengenai beberapa rancangan yang terdapat pada sistem berupa *use case diagram, activity diagram, dan class diagram*.

1. *Use Case Diagram*
   Use case diagram adalah pemodelan yang menggambarkan peranan pengguna pada sebuah sistem.
2. *Activity Diagram*
   Activity diagram merupakan gambaran aliran kerja dari menu menu yang terdapat pada sebuah sistem.
3. *Class Diagram*
   Class diagram merupakan gambaran aliran kerja pada struktur – struktur dalam membangun sebuah sistem.

5. PENGUJIAN DAN IMPLEMENTASI

Pengujian sistem merupakan kegiatan akhir dari penerapan sistem, dimana sistem akan mengoperasikan secara menyeluruh menggunakan metode *Advanced Encryption Standard*. Sebelum sistem digunakan, sistem harus diuji terlebih dahulu agar tidak adanya kendala yang muncul pada saat digunakan. Dalam pengujian program sistem pendukung keputusan untuk menentukan golongan perumahan membutuhkan 2 (dua) buah perangkat yaitu perangkat lunak (*Software*) dan perangkat keras (*Hardware*). Adapun perangkat lunak software dan perangkat keras hardware yang dibutuhkan yaitu sebagai berikut:

1. Perangkat Lunak (*Software)*

Perangkat Lunak (*Software*) yaitu merupakan program yang berisikan instruksi dalam pengoperasian komputer. Adapun perangkat Lunak yang dibutuhkan adalah sebagai berikut:

a. Sistem Operasi *Windows 7, Windows 8, Windows 10* atau sejenisnya.
b. *Microsoft Visual Studio* 2010.
c. *Microsoft Acces* 2007.
d. *Crystal Report 8.5*

2. Perangkat Keras (*Hardware)*

Sistem yang terkomputerisasi ini dapat dijalankan apabila telah dilakukan beberapa hal yaitu proses instalasi sudah dilakukan serta *hardware* yang mendukung dalam menjalankan program ini telah dipersiapkan. Spesifikasi *hardware* yang digunakan untuk mengimplementasikan sistem agar berjalan dengan baik adalah sebagai berikut:

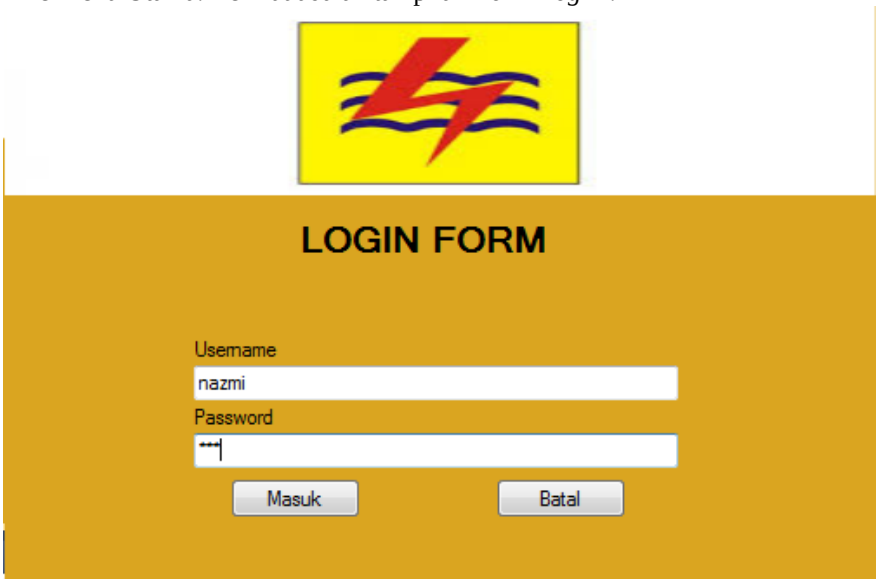
a. *Processor* Minimal *Intel Dual Core Processor.*
b. RAM *(Random Access Memory)* minimal 1 Gb.
c. *Keyboard.*
d. *Mouse.*

e. *Harddisk* minimal 100 Gb.

5.1 Implementasi Sistem

1. *Form Login*

Form Login digunakan untuk mengamankan sistem dari *user-user* yang tidak bertanggung jawab sebelum masuk ke Menu Utama. Berikut adalah tampilan *Form Login* :



Gambar 1 *Form Login*

Berikut keterangan pada gambar 1 *Form Login* :

a. Tombol login digunakan untuk mem-validasikan *username* dan *password* yang telah kita isi pada kotak teks yang disediakan.
b. Tombol Batal digunakan ketika kita batal melakukan *login* dan akan keluar dari sistem.
c. Link masuk sebagai pengunjung digunakan apa bila pengunjung ingin mencari rekomendasi terbaik untuknya.

2. *Form* Menu Utama

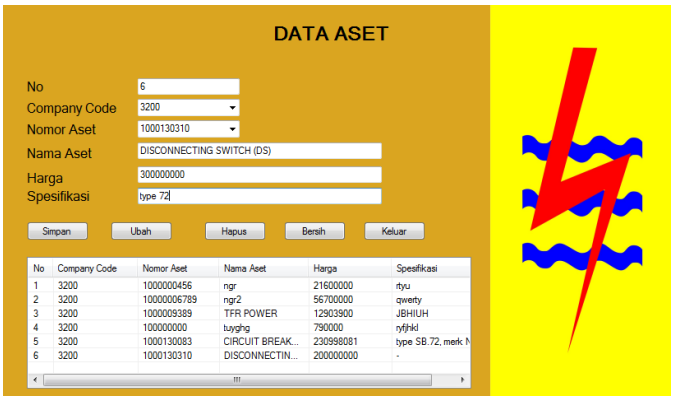
Form Menu Utama digunakan sebagai penghubung untuk *Form* Data *aset*, *Form* Proses *Enkripsi*, *Form Dekripsi*, dan *Form* Laporan. Selain itu, ada beberapa menu lainnya salah satunya ada menu *Keluar* bertujuan untuk mengakhiri program secara keseluruhan.

Gambar.2 *Form* Menu Utama

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

3. *Form* Data *aset*

Form Data *Aset* adalah *form* yang berfungsi untuk mengelola data Alternatif tentang *aset* dan akan diolah dengan Metode *Advanced Encryption Standard*. Berikut adalah tampilan hasil dari form data *aset*.



Gambar 3 *Form* Data *aset*

Berikut keterangan pada gambar 3 *form* Data *Aset*:

a. Tombol simpan digunakan ketika seluruh kotak teks telah terisi dan data dari kotak teks tersebut akan disimpan.
b. Tombol ubah digunakan untuk mengubah data yang telah tersimpan sebelumnya.
c. Tombol hapus digunakan untuk menghapus data yang terpilih pada daftar data yang ada.
d. Tombol keluar digunakan untuk keluar dari form.

4. *Form* Enkripsi

Form Enkripsi adalah *Form* yang digunakan untuk Mengamankan data customer. Berikut adalah tampilan form Enkripsi:

Gambar 4 *Form* Enkripsi

Berikut keterangan pada gambar 4 *form* Enkripsi:

a. Tombol Enkripsi digunakan untuk mengamankan data *customer* yang ada dengan menggunakan Algoritma *Advanced Encryption Standard.*
b. Tombol key generator untuk mencari generator kunci yang lain.
c. Tombol Cetak laporan digunakan untuk menampilkan laporan hasil enkripsi

5. *Form* Dekripsi

Form Dekripsi adalah *Form* yang digunakan untuk Mengubah data customer kembali seperti semula. Berikut adalah tampilan form Dekripsi:

Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475

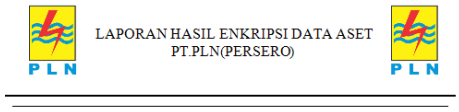
Gambar 5 *Form* Dekripsi

Berikut keterangan pada gambar 5 *form* Enkripsi:

a. Tombol Dekripsi digunakan untuk mengamankan data *customer* yang ada dengan menggunakan Algoritma *Advanced Encryption Standard*.
b. Tombol key generator untuk mencari generator kunci yang lain.
c. Tombol Cetak laporan digunakan untuk menampilkan laporan hasil dekripsi

6. *Form* Laporan

Form Laporan adalah *Form* yang digunakan untuk menampilkan hasil Enkripsi Data berdasarkan metode *Advanced Encryption Standard*. Berikut adalah tampilan form Laporan:



Nomor	Companycode	Nomoraset	Namaaset	Harga	Spesifikasi
xZg1PsfKeJDN b1zC6t+D+A=	JGUJ8V+NNf2/i DllIirucA==	+JD2wqd05GyrwCj5zbJP+A==	QrIoxSP+M9Rcbizt/dRpg==	OcWvWV0vstO/MItCUwZ5rg==	Hgm8NKrckHOvnIYQKa9vGg==
mFnZAcbw8qBYVK9b8StAOg==	JGUJ8V+NNf2/i DllIirucA==	nYeiC4KgutXyXIQGK6stuQ==	g8/dJJ2hldCEb9cG6pZ+PQ==	xoDeVOUOWOvfwbgFj86u9w==	yTHHYbk4yOKZb16x+iPvWw==
xTmG3IUi6/Mzcq D7cydTVw=	JGUJ8V+NNf2/i DllIirucA==	9zkyXVq9e30c2Usa2dk/4A==	eZm6fgruhyobFuSUdnN1MA==	ly2XOgo5wgXL8eZzYl82ig==	aw11mj2gmUWix6lPM2b7DQ==
cSjxwl2fH6QX9tS3S7ExjA==	JGUJ8V+NNf2/i DllIirucA==	yEs9BHQXt0Hci0WeJzW8iA==	O5eZ7v93CCuncB1ME2NKoA==	tcn1afoNY8uGEgMoG61mqQ==	7St/gQnuX8+x4jA9qCfL/g==
SUrdExw34TLoBECF79MOiA==	JGUJ8V+NNf2/i DllIirucA==	345Dbi0+gRqbg+/W5IVNtA==	ZiK5vFtugb1wYVkKlbpktcX1H+rL94QZ9dsNnvo9	jgoy6vJjZ3ssAH0w0pO+kg==	xn2GF72vnNa5zyf3XoZeJ64T0g6QZGTTLq/zOstc

Gambar 6 *Form* Laporan

5.2 Kelebihan dan Kelemahan Sistem

Setelah melakukan proses penerapan dan pengujian terhadap sistem, algoritma Rivest Shamir Adleman dan Caesar Cipher ini mempunyai beberapa kelebihan dan kelemahan terhadap sistemnya, dimana sistem ini masih memerlukan pengembangan secara bertahap. Berikut kelebihan dan kelemahan dari sistem ini adalah :

1. Kelebihan Sistem
   a. Dapat mengamankan data dalam database dengan sistem pengamanan data yang cukup rumit.
   b. Proses pengamanan data yang rumit, dapat diubah menjadi sederhana dan spesifik.

c. Aplikasi pengamanan data ini dapat membantu pengguna atau pihak Jeje Olshop untuk lebih mudah dalam mengamankan data *aset*.
d. Aplikasi yang telah dibangun ini dapat digunakan pada perusahaan lain karena fungsinya untuk mengamankan *database* yang penting.

1. Kelemahan Sistem
   a. Aplikasi pengamanan data yang telah dibangun ini hanyalah membahas tentang pengamanan data pada *database*.
   b. Pada sistem ini belum memiliki fasilitas *backup* data, apabila data hilang atau terhapus maka datanya tidak dapat dikembalikan kedalam bentuk semula.
   c. Dalam proses pengamanan data masih berbasis desktop sehingga dalam proses mengakses data cukup sulit untuk diakses pihak PT.PLN .

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan penelitian yang telah dilalui dalam tahap perancangan dan evaluasi kriptografi dalam mengamankan data *customer* pada Jeje Olshop dengan menggunakan algoritma *Advanced Encryption Standard* maka dapat disimpulkan bahwa:

1. Untuk mengamankan data *aset* PT.PLN medan yang bersifat rahasia akan diamankan menggunakan algoritma kriptografi *Advanced Encryption Standard*.
2. Algoritma Rivest Shamir Adleman(RSA) dan Caesar Cipher digunakan sebagai sistem dalam pengamanan data yang merupakan algoritma yang cukup rumit dalam perhitungannya untuk mengamankan data yang cukup banyak sehingga dapat mengurangi resiko dalam penyalahgunaan data *aset* dan dapat mengoptimalkan dalam pengamanan data untuk mengamankan data *aset* pada PT.PLN.
3. Dengan cara merancang sistem aplikasi yang dapat digunakan dalam mengamankan data *aset* dan mengenkripsi data menjadi karakter sehingga dapat mengamankan data dengan maksimal dan baik.

6.2 Saran

Adapun saran-saran yang dapat disampaikan kepada pembaca dan kepada seluruh pihak yang berkaitan dengan perancangan sistem ini, yaitu:

1. Diharapkan dalam penelitian yang selanjutnya dapat dikembangkan dengan menggabungkan algoritma yang lain sehingga dapat meningkatkan kinerja sistem.
2. Kepada PT.PLN yang akan menggunakan sistem ini harus diberikan pelatihan untuk pengoperasiannya. Hal ini disampaikan agar penggunaan sistem ini dapat lebih maksimal dan menghindari kesalahan yang tidak diinginkan.
3. Sistem ini masih dibuat hanya untuk Jeje Olshop, disarankan agar sistem ini juga dapat di gunakan untuk perusahaan lainnya.

UCAPAN TERIMA KASIH

Pada kesempatan ini saya ucapkan terimakasih kepada Bapak, Ibu dan keluarga saya atas segala doa, semangat dan motivasinya. Selain itu, terimakasih sebesar-besarnya kepada semua pihak yang telah membantu untuk menyelesaikan penulisan skripsi ini, yaitu :

1. Bapak Rudi Gunawan, SE, M.Si, Selaku Ketua STMIK Triguna Dharma Medan.
2. Bapak Dr. Zulfian Azmi, ST, M.Kom Selaku Wakil Ketua I Bidang Akademik STMIK Triguna Dharma Medan.
3. Bapak Marsono. S.Kom, M.Kom, Selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma Medan.
4. Bapak Nurcahyo Budi Nugroho, S.Kom, M.Kom selaku Dosen Pembimbing I yang membimbing dan menyediakan waktu selama ini.
5. Ibu Widiarti Ristamaya, ST., MM selaku Dosen Pembimbing II yang membimbing dan menyediakan waktu selama ini.
6. Seluruh Dosen, Staff dan Pegawai STMIK Triguna Dharma.
7. Terimakasi juga disampaikan kepada PT. PLN Medan yang telah mengizinkan melakukan penelitian dan memberikan data yang benar sehingga skripsi ini dapat terselesaikan dengan baik.

Akhir kata saya ucapkan rasa terima kasih kepada semua pihak yang terlibat dalam penyelesaian skripsi ini Skripsi ini masih sangat jauh dari sempurna. Oleh karena itu, diharapkan saran dan kritik yang sifatnya membangun dari para pembaca demi kesempurnaan skripsi ini.

REFERENSI

[1] D. Kurniawan, R. Afyenni and R. Hidayat, "PROSIDING SEMINAR NASIONAL SISFOTEK (Sistem Informasi dan Teknologi) Implementasi Algoritma AES dalam Mengenkripsi Berkas Terintegrasi dengan Layanan Cloud Storage Berbasis Android".

[2] L. A. Indrayani and I. M. Suartana, "Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document," 2019.

[3] "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital," Yusuf Anshori, vol. 18, Mei 2019.

[4] "Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma Rsa Dengan Metode Waterfall Berbasis Java," *Rudi Firmansyah*, vol. 4, p. 1, 2019.

[5] "Pembangunan Aplikasi Pembanding Kriptografi Dengan Caesar Cipher Dan Advance Encryption Standard (Aes) Untuk File Teks," Aji Fitrah Marisman, vol. 19, p. 1, Desember 2015.

Data Diri

Nama	: Nazmi May Sarah Sianturi
Tempat/Tanggal Lahir	: Medan, 06 Mei 1997
Jenis Kelamin	: Perempuan
Agama	: Islam
Status	: Belum Menikah
Pendidikan Terakhir	: Sekolah Menengah Kejuruan
Kewarganegaraan	: Indonesia
E-mail	: nazmimaysarah00@gmail.com

Pendidikan Formal

1. Tahun 2004 - 2010 : SD Yapena 45 Medan
2. Tahun 2010 -2013 : SMP Negeri 2 Medan
3. Tahun 2013 -2015 : SMK Negeri 7 Medan

Nurcahyo Budi Nugroho, S.Kom., M.Kom
Beliau merupakan dosen pengajar tetap di STMIK Triguna Dharma.
E-mail : nurcahyobn@gmail.com

Widiarti Ristamaya, ST, M.Kom
Beliau merupakan dosen pengajar tetap di STMIK Triguna Dharma.
E-mail : widiartirm78@gmail.com