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

Penerapan Kriptografi Menggunakan Algoritma AES untuk Keamanan Data Penjualan P ada PT.Mestika Sakti

Muhammad Arif Hidayah[*], Nurcahyo Budi Nugoho[**], Moch. Iswan Perangin-Angin [**]
[*] Program Studi Sistem Informasi, STMIK Triguna Dharma
[**] Program Studi Sistem Informasi, STMIK Triguna Dharma

Article Info
Article history:

Keyword:
Kriptografi, Advanced Encryption Standard (AES), AES 128bit,

ABSTRACT

PT.Mestika Sakti Medan merupakan perusahaan farmasi atau perusahaan obat – obatan yang lebih terfokus untuk mendistribusikan obat. Distribusi sendiri merupakan kegiatan pemasaran yang fungsinya mempermudah kegiatan pengiriman atau penyampaian barang atau jasa dari pihak produsen ke pihak konsumen. Seiring perkembangan teknologi, hal tersebut memiliki dampak negatif berupa pencurian atau manipulasi data. Sehingga aspek keamanan pada dokumen sangat penting.[3]

Dokumen rahasia perusahaan akan merugikan perusahaan apabila jatuh ke pihak yang tidak berhak untuk disalahgunakan. Karena terdapat pihak yang tidak berhak untuk disalagunakan. Karena hal tersebut, diperlukan suatu aplikasi pengamanan data tersebut, aplikasi pengamanan data yang bisa mengamankan suatu data serta tidak menimbulkan kecurigaan oleh pihak yang tidak berhak.[4]

Pada permasalahan yang dibahas, dapat menerapkan Perancangan Aplikasi Keamanan Data salah satunya ialah menggunakan algoritma Advanced Encryption Standard (AES).

Hasil penelitian merupakan terciptanya sebuah aplikasi Pengamanan Data dengan Advanced Encryption Standard (AES) yang dapat membantu dalam mengamankan data penjualan pada PT. Mestika Sakti.

First Author
Nama : Muhammad Arif Hidayah
Program Studi : Sistem Informasi STMIK Triguna Dharma
Email : Muhammadarifhidayah82@gmail.com

1. PENDAHULUAN

Seiring perkembangan ilmu pengetahuan dan teknologi dalam bidang kefarmasian serta semakin tingginya kesadaran masyarakat dalam meningkatkan kesehatan, maka dituntut juga kemampuan dan kecakapan para petugas dalam angka mengatasi permasalahan yang mungkin timbul dalam pelaksanaan pelayanan kefarmasian kepada masyarakat.[1] Dengan demikian banyak perusahaan farmasi di Indonesia yang memproduksi obat dan alat kesehatan dengan kegunaan yang sama sehingga persaingan antar perusahaan farmasi menjadi sangat ketat.[2]

PT.Mestika Sakti Medan merupakan perusahaan farmasi atau perusahaan obat – obatan yang lebih terfokus untuk mendistribusikan obat. Kegiatan distribusi ini juga membantu perusahaan dalam meningkatkan proses penjualan.[3]

Kriptografi adalah sebuah seni untuk memanipulasi suatu pesan maupun data rahasia ke dalam bentuk yang tidak diketahui oleh banyak orang dengan tujuan pesan atau data rahasia tersebut terlindungi dari orang yang tidak berhak mengetahuinya. [6]

Algoritma AES merupakan algoritma simetris yaitu mengunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256 .[14]
Berdasarkan masalah yang dihadapi, maka penulis mengangkat judul sebagai inti pembahasan dalam penelitian yaitu **"Penerapan kriptografi menggunakan algoritma AES untuk keamanan data penjualan pada PT.Mestika Sakti"**

2. KAJIAN PUSTAKA

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, *Crypto* dan Graphia. *Crypto* berarti rahasia (*secret*) dan graphia berarti tulisan (*writing*).[5] Konsep dasar kriptografi berlandaskan pada teori-teori yang ada dalam ilmu matematika, seperti penguraian bilangan yang sangat besar, komputasi logaritma diskrit, teknik-teknik yang bersifat probabilistik dan lain sebagainya. Teori-teori inilah yang membuat kriptografi menjadi aman digunakan untuk mengirimkan pesan yang bersifat rahasia.[6]

2.2 Advanced Encryption Standard (AES)

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.

2.3 Algoritma Advanced Encryption Standard (AES)

Adapun algoritma penyelesaian metode AES yaitu sebagai berikut:

1. *AddRoundKey*: melakukan XOR antara *state* awal (*plaintext*) dengan *cipher key*. Tahap ini disebut juga *initial round*
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. *SubBytes* : *substitusi byte* dengan menggunakan *table substitusi* (S-box).
   b. *ShiftRows* : pergeseran baris-baris *array state* secara *wrapping.*
   c. *MixColumns* : mengacak data di masing-masing kolom *array state.*
   d. *Add Round Key* : melakukan XOR antara *state* sekarang *round key*.
3. *Final round* : proses untuk putaran terakhir:
   a. SubBytes
   b. ShiftRows
   c. MixColumns
   d. Add Round Key

METODOLOGI PENELITIAN

Metode penelitian yang digunakan akan menentukan keabsahan hasil penelitian. Metode penelitian bukan hanya statistik apa yang akan digunakan, namun lebih kepada pemikiran di balik penelitian yaitu bagaimana peneliti benar-benar ingin mencari tahu, bagaimana membangun argumen tentang ide-ide dan konsep, dan apa bukti bahwa peneliti dapat menemukan argument atau mendukung argumen yang telah ada.

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
   Dalam penelitian ini dilakukan observasi pra-riset telebih dahulu untuk mencari masalah yang terjadi di PT.Mestika Sakti terkhusus dalam pengamanan data, dari masalah tersebut akan dirumusakan dalam penelitian ini sehingga dapat menemukan rumusan apa saja yang perlu dipersiapkan untuk bagaimana cara menyelesaikan masalah tersebut.
b. Wawancara
   Setelah itu dilakukan wawancara kepada pemilik perusahaan PT.Mestika Sakti yang mempunyai andil dalam pengelolaan data. Serta mencari solusi untuk kendala yang dihadapi oleh bagian pengamanan data itu sendiri selama ini

2. *Studi Literatur*

Didalam studi literatur, tahap ini dilakukan cara pengumpulan data dengan mencari berbagai jurnal, buku dan modul yang berkaitan dengan Kriptografi, dengan algoritma *Advanced Encryption Standard (AES)*.

3.1 Metode Perancangan 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*). 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

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

Algoritma *Advanced Encryption Standard* (AES) mengenkripsi 128-bit blok *plaintext* (M), menjadi 128-bit blok *chipertext* (C), menggunakan kunci chiper (chiper *key* K) yang panjangnya diantara 128-bit, 192-bit, atau 256-bit. Perbedaan dari panjang kunci mejadikan nama kunci AES-128, AES-192, dan AES-256, berikut ini adalah langkah-langkah penyelesaian metode *Advanced Encryption Standard* (AES):

1. Proses Ekspansi Kunci
2. Proses Enkripsi.
3. Transformasi MixColumns.
4. Langkah terakhir untuk mendapatkan enkripsi putaran pertama dengan melakukan XOR.
5. Proses Dekripsi

3.2.1 Penyelesaian

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

Tabel 3.1 Sampel Data *Customer* di Jeje Olshop Medan

Tanggal	No. Faktur	Nama Perusahaan	Alamat	Nama Produk	Qty. (Unit)	Harga @	Sub Total [Tr]
04/04/2019	LAP.0419.001	JUANG FARMA. APT	JL. T.UMAR JOHAN PAHLAWAN NO.150	INFLASON/20X10KAPLET	100	31713	3171300

3.3.3 Penyelesaian Masalah Dengan Algoritma *Advanced Encryption Standard* (AES)

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

3.3.3.1 Proses Enkripsi Algoritma *Advanced Encryption Standard* (AES)

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 128 bit (16 kode ASCII). Lalu ubah kunci kedalam bentuk heksadecimal

d	a	t	a	p	e	n	j	u	a	l	a	n	o	b	t
64	61	74	61	70	65	6E	6A	75	61	6C	61	6E	6F	62	74

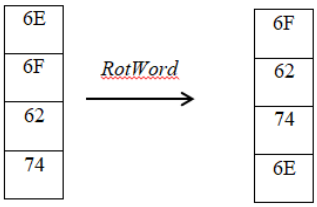
b. Langkah selanjutnya yaitu susun kunci yang telah diubah kedalam bentuk heksadesimal kedalam state berukuran 4 × 4 seperti dibawah ini :

64	70	75	6E
61	65	61	6F
74	6E	6C	62
61	6A	61	74

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.

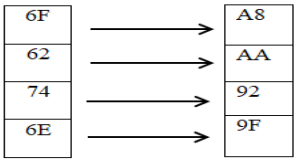
Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475



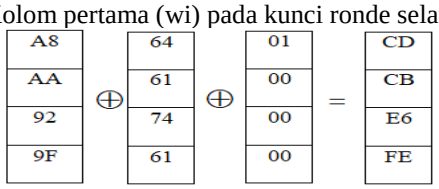
d. Kemudian hasil dari *RotWord* tersebut disubtitusikan dengan nilai pada tabel *S-Box* (*SubBytes*).

Tabel 3.3 *S-Box (SubBytes)*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

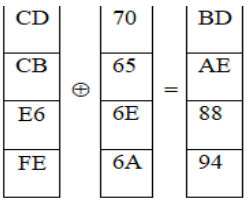


e. Tahap yang terakhir yaitu lakukan proses *XOR* antara kolom pertama dari kunci *ronde* ke-0, hasil dari *SubBytes* lalu di-*XOR*-kan lagi dengan *RCon*. Kolom pertama (wi) pada kunci ronde selanjutnya (ronde ke-1) = K1

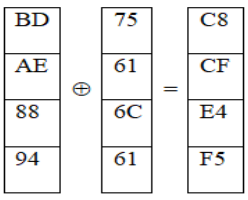


f. Untukmendapatkan kolom kedua, diperoleh dari proses *XOR* antara Wi dengan kolom kedua dari kunci ronde ke-0. Sedangkan untuk mendapatkan kolom ketiga dan keempat kunci ronde ke-1, dilakukan proses seperti memperoleh kolom kedua.

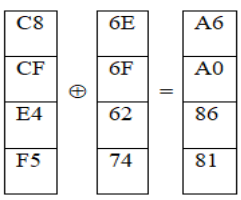
Kolom ke-2



Kolom ke-3



Kolom ke-4



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

CD	BD	C8	A6
CB	AE	CF	A0
E6	88	E4	86
FE	94	F5	81

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:

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

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

RoundKey Ke-1

CD	BD	C8	A6
CB	AE	CF	A0
E6	88	E4	86
FE	94	F5	81

RoundKey Ke-2

2F	92	5A	FC
8F	21	EE	4E
EA	62	86	00
DA	4E	BB	3A

RoundKey Ke-3

04	96	CC	30
EC	CD	23	6D
6A	08	8E	8E
6A	24	9F	A5

RoundKey Ke-4

30	A6	6A	5A
F5	38	1B	76
6C	64	EA	64
6E	4A	D5	70

RoundKey Ke-5

18	BE	D4	8E
B6	8E	95	E3
3D	59	B3	D7
D0	9A	4F	3F

RoundKey Ke-6

29	97	43	CD
B8	36	A3	40
48	11	A2	75
C9	53	1C	23

RoundKey Ke-7

60	F7	B4	79
25	13	B0	F0
6E	7F	DD	A8
74	27	3B	18

RoundKey Ke-8

6C	9B	2F	56
E7	F4	44	B4
C3	BC	61	C9
C2	E5	DE	C6

RoundKey Ke-9

FA	61	4E	18
3A	CE	8A	3E
77	CB	AA	63
73	96	48	8E

RoundKey Ke-10

7E	1F	51	49
C1	0F	85	BB
6E	A5	0F	6C
DE	48	00	8E

2. Proses Enkripsi
   Plaintext yang akan digunakan adalah"PT.MESTIKA SAKTI

P	T	.	M	E	S	T	I	K	A		S	A	K	T	I
70	74	2E	6D	65	73	74	69	6B	61	20	73	61	6B	74	69

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

70	65	6B	61
74	73	61	6B
2E	74	20	74
6D	69	73	69

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

70	65	6B	61
74	73	61	6B
2E	74	20	74
6D	69	73	69

$\oplus$

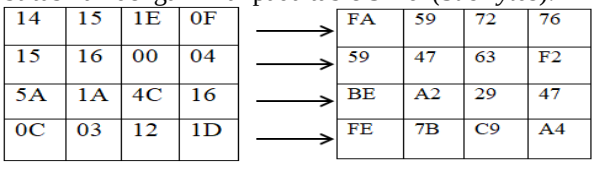
64	70	75	6E
61	65	61	6F
74	6E	6C	62
61	6A	61	74

=

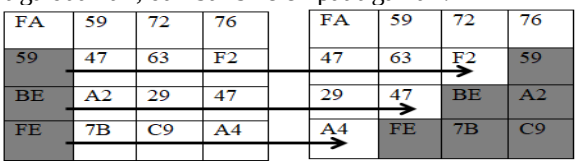
14	15	1E	0F
15	16	00	04
5A	1A	4C	16
0C	03	12	1D

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*.

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

$sb0.a_0$ = (FA).(02)
= (11111010) .(10)
= $(x^7+x^6+x^5+x^4+x^3+x)$. (x)
= $x^7+x^6+x^5+x^3+x^2+x+1$
= 11101111
a_1 = (47) .(03)
= (01000111) . (11)
= (x^6+x^3+x+1) . (x+1)
= $x^7+x^6+x^3+1$
= 11001001
a_2 = (29) . (1) = 00101001
a3 = (A4) . (1) = 10100100
b_0 = 11101111 xor 11001001 xor 00101001 xor 10100100 = 10101011 = AB.
b_1= (FA.01)xor(47.02)xor(29.03)xor(A4.01) = 10101011 = AB.
b_2= (FA.01)xor(47.01)xor(29.02)xor(A4.03) = 00011000 = 18.
b_3= (FA.03)xor(47.01)xor(29.01)xor(A4.02) = 00101000 =28.
Lakukan perulangan seperti yang diatas,sehingga di dapatkan hasil *MixColumns* seperti sebagaiberiku
.

FA	59	72	76
47	63	F2	59
29	47	BE	A2
A4	FE	7B	C9

→

AB	AE	2C	6C
AB	A8	2F	F0
18	AD	6A	30
28	28	2C	E8

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

MixColumns

AB	AE	2C	6C
AB	A8	2F	F0
18	AD	6A	30
28	28	2C	E8

⊕ *Roundekey* ke-1

CD	BD	C8	A6
CB	AE	CF	A0
E6	88	E4	86
FE	94	F5	81

= *AddRoundeKey*

66	13	E4	CA
60	06	E0	50
FE	25	8E	B6
D6	BC	D9	69

Lakukan proses diatas sampai 10 kali putaran (*rounde*). Berikut adalah hasil enkripsi hingga *rounde* ke-10.

Rounde ke-1

66	13	E4	CA
60	06	E0	50
FE	25	8E	B6
D6	BC	D9	69

Rounde ke-2

18	E8	A3	75
B0	A1	92	F5
94	63	7E	85
10	91	22	23

Rounde ke-3

C6	37	4A	4B
0D	A0	19	A0
62	AC	BE	B7
0B	C5	5C	38

Rounde ke-4

D1	6C	EA	9E
74	DA	55	92
76	1E	62	E7
E9	D4	A9	6C

Rounde ke-5

67	8B	60	94
93	84	8C	92
EB	E4	D3	C4
CF	3E	3A	7F

Rounde ke-6

6D	D7	72	1F
FB	6D	7F	FA
33	F5	39	C2
DB	63	AE	EB

Rounde ke-7

A7	1A	7B	F1
BE	74	0F	FB
6A	39	3B	87
D7	AB	F8	79

Rounde ke-8

2D	47	1C	B5
0F	8D	1F	25
13	54	ED	21
21	65	74	00

Rounde ke-9

80	61	1C	81
C4	14	A2	F5
FD	56	24	2D
CE	B1	2F	83

Rounde ke-10

B3	F0	CD	45
3B	35	63	A7
58	7D	5B	DD
32	C3	C8	9B

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

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

Tabel 3.4 *rounde* kode ASCII untuk *Ciphertext*

Rounde	Kode ASCII	Karakter
B3	179	³
3B	59	;
58	88	X
32	50	2
F0	240	ð
35	53	5
7D	125	}
C3	195	Ã
CD	205	Í
63	99	c
5B	91	[
C8	200	È
45	69	E
A7	167	§
DD	221	Ý
9B	155	

Dan hasil dari enkripsi dengan algoritma AES menghasilkan Ciphertext sebagai berikut:

179,59,88,50,240,53,125,195,205,99,91,200,69,167,221,155

3.3.3.4 Proses Dekripsi Algoritma Algoritma *Advanced Encryption Standard* (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.

B3	3B	58	32	F0	35	7D	C3	CD	63	5B	C8	45	A7	DD	9B

Kemudian susun 16 byte pertama dari *ciphertext* yang telah diubah ke bentuk hexadesimal ke dalam *state* 4x4:

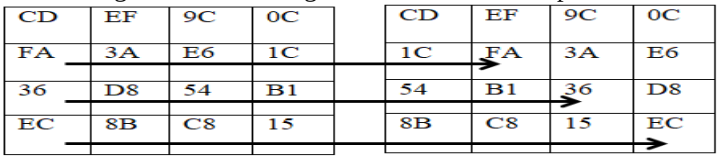
B3	F0	CD	45
3B	35	63	A7
58	7D	5B	DD
32	C3	C8	9B

Lakukan *XOR* antara *Ciphertext* dengan *RoundKey* 10. Proses ini dinamakan *AddInvRoundKey*.

B3	F0	CD	45	⊕	7E	1F	51	49	=	CD	EF	9C	0C
3B	35	63	A7		C1	0F	85	BB		FA	3A	E6	1C
58	7D	5B	DD		6E	A5	0F	6C		36	D8	54	B1
32	C3	C8	9B		DE	48	00	8E		EC	8B	C8	15

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*,

1. 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.



2. Hasil dari *InvShiftrows* disubtitusikan dengan nilai pada tabel *S-Box*$^{-1}$ *(InvSubBytes).*

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

Tabel 3.5 *InvSubBytes*

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

CD	EF	9C	0C
1C	FA	3A	E6
54	B1	36	D8
8B	C8	15	EC

→

80	61	1C	81
C4	14	A2	F5
FD	56	24	2D
CE	B1	2F	83

3. XOR hasil dari *InvSubBytes* dengan *RoundKey* ke-9. Proses ini disebut *AddInvRoundKey*.

80	61	1C	81	⊕	FA	61	4E	18	=	7A	00	52	99
C4	14	A2	F5		3A	CE	8A	3E		FE	DA	28	CB
FD	56	24	2D		77	CB	AA	63		8A	9D	8E	4E
CE	B1	2F	83		73	96	48	8E		BD	27	67	0D

4. 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*.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

$S_{0.0}$ = (0E).(7A)
= (1110).(01111010)
= $(x^3+x^2+x).(x^6+x^5+x^4+x^3+x)$
= $x^7+x^6+x^5+x^4+x^3+x$ = 1111 1010 = FA

$S_{1.0}$ = (0B).(FE)
= (1011).(11111110)
= $(x^3+x+1).(x^7+x^6+x^5+x^4+x^3+x^2+x)$
= $x^7+ x^5 +x^3$ = 1010 1000 = A8

$S_{2.0}$ = (0D).(8A)
= (1101).(10001010)
= $(x^3+x^2+1).(x^7 +x^3+x)$
= $x^7+x^5+x^3$ = 1010 1000 =A8

$S_{3.0}$ = (09).(BD)
= (1001).(10111101)
= $(x^3+1).(x^7+x^5+x^4+x^3+x^2+1)$
= $x^5 +x$ = 0010 0010 = 22

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

7A	00	52	99
FE	DA	28	CB
8A	9D	8E	4E
BD	27	67	0D

→

D8	A0	9C	D5
5D	C0	3F	76
55	FD	7D	20
63	FD	4D	92

Proses diatas diulang sampai 10 kali putaran (*round*). Berikut adalah hasil dari dekripsi hingga *round* ke-10.

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

Rounde ke-1

D8	A0	9C	D5
5D	C0	3F	76
55	FD	7D	20
63	FD	4D	92

Rounde ke-2

5C	A2	21	A1
92	76	0F	AE
E2	17	02	12
B6	0E	62	41

Rounde ke-3

3C	0E	40	C0
3C	D2	2D	0F
12	25	C3	E6
E9	B9	FB	E4

Rounde ke-4

85	3D	D0	22
5F	64	4F	DC
66	1C	E9	69
D2	8A	B2	80

Rounde ke-5

3E	50	87	0B
57	FC	4F	92
AA	94	38	72
50	1E	48	D3

Rounde ke-6

B4	9A	D6	B3
E0	D4	E0	D7
AE	A9	AA	91
07	2B	A6	4A

Rounde ke-7

AD	9B	0A	9D
32	4F	E6	E7
F3	97	22	FB
26	CA	81	93

Rounde ke-8

33	7D	69	74
6F	E1	53	D0
19	4E	BB	3F
F9	F6	65	35

Rounde ke-9

FA	59	72	76
47	63	F2	59
29	47	BE	A2
A4	FE	7B	C9

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

InvShiftrows

FA	59	72	76
47	~~63~~	~~F2~~	~~59~~
29	~~47~~	~~BE~~	~~A2~~
A4	~~FE~~	~~7B~~	~~C9~~

→

FA	59	72	76
~~59~~ → 47	63	F2	
~~BE~~ → 29	~~A2~~	47	
~~FE~~	~~7B~~	~~C9~~ → A4	

InvSubBytes

FA	59	72	76
59	47	63	F2
BE	A2	29	47
FE	7B	C9	A4

→

14	15	1E	0F
15	16	00	04
5A	1A	4C	16
0C	03	12	1D

AddInvRoundKey

14	15	1E	0F
15	16	00	04
5A	1A	4C	16
0C	03	12	1D

⊕

64	70	75	6E
61	65	61	6F
74	6E	6C	62
61	6A	61	74

=

70	65	6B	61
74	73	61	6B
2E	74	20	74
6D	69	73	69

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

Tabel 3.6 *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

Tabel 3.6 *rounde* kode ASCII dan karakter untuk *Plaintext*

Rounde	Kode ASCII	Karakter
61	97	A
6B	107	K
74	116	T
69	105	I

Dan hasil dari dekripsi dengan algoritma AES menghasilkan *Plaintext*.

4. PEMODELAN SISTEM DAN PERANCANGAN

Pemodelan merupakan salah satu teknik yang digunakan untuk menggambarkan bagaimana sistem informasi akan dibuat dan dihasilkan. Pemodelan sendiri dapat dijadikan acuan dalam proses pengembangan sistem infromasi agar sesuai dengan kebutuhan pengguna.

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 adalah pemodelan untuk kelakuan sistem informasi yang akan dibuat dari suatu sistem sehingga *costumer* atau pengguna sistem paham dan mengerti mengenai kegunaan sistem yang akan dibangun.
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 *Weighted Product.* 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* 20010.
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:

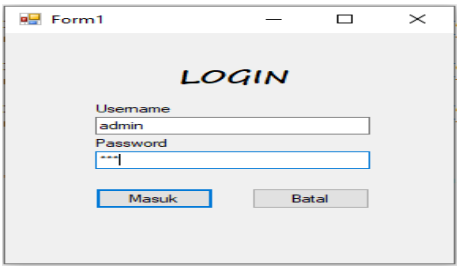
a. *Processor* Minimal *Intel Dual Core Processor.*
b. RAM *(Random Access Memory)* minimal 1 Gb.
c. *Keyboard.*
d. *Mouse.*
e. *Harddisk* minimal 500 Gb.

5.1 Implementasi Sistem

1. *Form Login*

Sebelum masuk dan mengakses aplikasi, *user* harus melakukan *login* terlebih dahulu dengan cara meng-*input user name* dan *password* dengan benar sesuai dengan sistem *database* dan akan masuk ke menu utama, namun jika tidak maka harus mengulangi untuk meng-*input user name* dan *password* dengan benar. Di bawah ini merupakan tampilan *form login* adalah sebagai berikut:

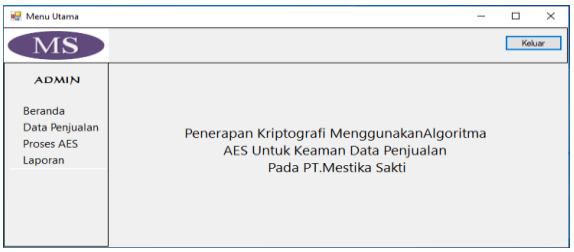
Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475



Gambar 5.1 *Form* Login

2. *Form* Menu Utama

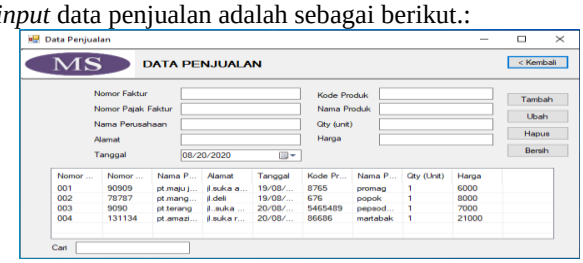
Halaman menu utama merupakan tampilan halaman awal sistem untuk melakukan pengolahan data di dalam Mengamankan Data penjualan pada PT.Mestika Sakti Menggunakan Algoritma *Advanced Encryption Standard* (AES). Di bawah ini merupakan tampilan halaman menu utama adalah sebagai berikut :



Gambar 5.2 *Form* Menu Utama

3. *Form* Data Penjualan.

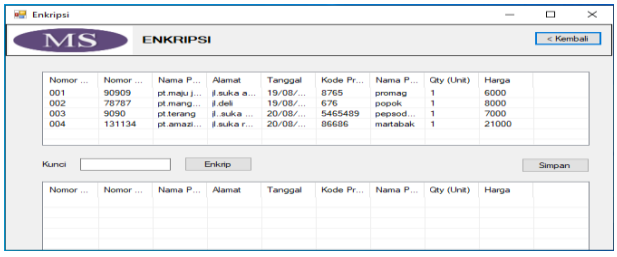
Form data penjualan merupakan *form* yang digunakan untuk meng-*input* data penjualan PT.Mestika Sakti. Di bawah ini merupakan tampilan *form input* data penjualan adalah sebagai berikut.:



Gambar 5.3 *Form* Data Penjualan.

4. *Form* Enkripsi

Form Enkripsi merupakan *form* yang digunakan untuk mengubah data penjualan yang ada pada PT.Mestika Sakti. Di bawah ini merupakan tampilan *form* Enkripsi adalah sebagai berikut

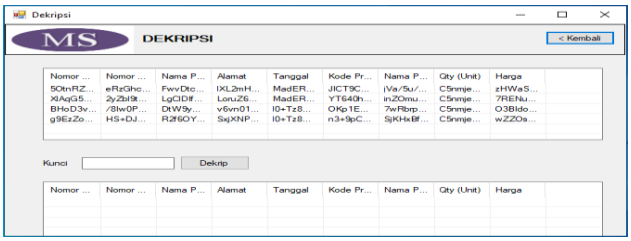


Gambar 5.4 *Form* Enkripsi

5. *Form* Dekripsi

Form Dekripsi merupakan *form* yang digunakan untuk mengubah data kembali seperti awal yang ada pada PT.Mestika Sakti. Di bawah ini merupakan tampilan *form* dekripsi adalah sebagai berikut

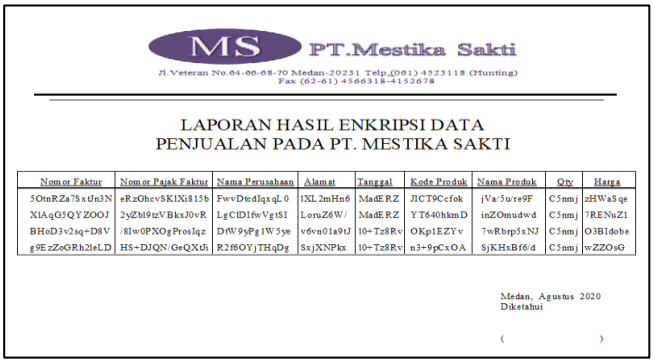
Jurnal CyberTech
Vol.x. No.x, Juli 2020, pp. xx~xx
P-ISSN : 1978-6603
E-ISSN : 2615-3475



Gambar 5 *Form* Dekripsi

6. *Form* Laporan

Form Laporan digunakan untuk menampilkan hasil proses perubahan data pada data penjualan dengan menggunakan algoritma *Advanced Encryption Standard* (AES). Di bawah ini merupakan tampilan *form* Laporan Pengamanan Data menggunakan algoritma *Advanced Encryption Standard* (AES):



Gambar 6 *Form* Laporan

5.2 Kelebihan dan Kelemahan Sistem

Setelah melakukan proses penerapan dan pengujian terhadap sistem, algoritma *Advanced Encryption Standard* (AES) 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 PT. Mestika Sakti untuk lebih mudah dalam mengamankan data penjualan..
   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. Mestika Sakti.

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan penelitian yang telah dilalui dalam tahap perancangan dan evaluasi kriptografi dalam mengamankan data Penjualan pada PT.Mestika Sakti dengan menggunakan algoritma *Advanced Encryption Standard(AES)* maka dapat disimpulkan bahwa:

1. Untuk mengamankan data Penjualan PT.Mestika Sakti Medan yang bersifat rahasia akan diamankan menggunakan algoritma kriptografi *Advanced Encryption Standard(AES)*.
2. *Advanced Encryption Standard(AES)* 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 Penjualan dan dapat mengoptimalkan dalam pengamanan data untuk mengamankan data Penjualan pada PT.Mestika Sakti.

3. Dengan cara merancang sistem aplikasi yang dapat digunakan dalam mengamankan data Penjualan dan mengenkripsi data menjadi karakter sehingga dapat mengamankan data dengan maksimal dan baik.
4. Dengan sistem yang telah dibangun menggunakan aplikasi *Visual Studio* pada kriptografi dalam pengamanan data menggunakan algoritma *Advanced Encryption Standard(AES)*, Sehingga sistem ini mampu membantu dalam mengamankan data Penjualan PT.Mestika Sakti .

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. Mestika Sakti 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 PT. Mestika Sakti, 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. Bapak Moch.Iswan Perangin-angin, S.Kom, M.Kom 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. Mestika Sakti 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] A. N. Putra, T. Septian, and A. W. Sudrajad, "Sistem Informasi Pendistribusian Obat Berbasis Web Pada Pt . Mersi Farma," no. x, pp. 1–13, 2019.

[2] P. Masyarakat, T. Tayangan, and S. Kopi, "hubungan antara adversity quotient dengan komitmen organisasi pada medical representative," no. x, pp. 84–90, 2017.

[3] F Fahira, "Peranan HPP (Harga Pembelian Pemerintah) terhadap Kegiatan Distribusi Beras pada PERUM BULOG Sumatera Barat," vol. 3, no. September, pp. 1–47, 2019.

[4] R. Rahmawati and D. Rahardjo, "Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi grafi AES 128 BIT pada SMK PGRI 15 Jakarta," J. Tek. Inform. dan Sist. Inf., vol. 2, no. April, pp. 67–74, 2016.

[6] A. Hybrid, K. Rsa, D. Kriptografi, and O. N. E. Time, "Muhammad Ghiyats Ristiana, 2017 ALGORITMA HYBRID KRIPTOGRAFI RSA DENGAN KRIPTOGRAFI ONE TIME PAD Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu," pp. 1–4, 2019.

[14] A. Rachman, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," vol. 3, no. 2, pp. 112–115, 2018.

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

Data Diri

Nama	: Muhammad Arif Hidayah
Tempat/Tanggal Lahir	: Medan, 17 September 1996
Jenis Kelamin	: Laki Laki
Agama	: Islam
Status	: Belum Menikah
Pendidikan Terakhir	: Sekolah Menengah Kejuruan
Kewarganegaraan	: Indonesia
E-mail	: muhammadarifhidayah82@gmail.com

Nurcahyo Budi Nugroho, S.Kom., M.Kom
Beliau merupakan dosen pengajar tetap di STMIK Triguna Dharma.

Moch.Iswan Perangin-Angin, S.kom, M,kom
Beliau merupakan dosen pengajar tetap di STMIK Triguna Dharma.