Jurnal CyberTech

Vol.x. No.x, September 2020, pp. xx~xx

P-ISSN : xxxx-xxxx

E-ISSN : xxxx-xxxx

Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. MITSUBISHI ELECTRIC INDONESIA.

Fandi Ahmad Sitorus *, Nurcahyo Budi Nugroho**, **Usti Fatimah Sari Sitorus Pane ****

* Program Studi Mahasiswa, STMIK Triguna Dharma

** Program Studi Dosen Pembimbing, STMIK Triguna Dharma

Article Info

Article history:

Received Jun 12th, 2020

Revised Aug 20th, 2020

Accepted Aug 26th, 2020

Keyword:

Kriptografi AES 128 Bit

ABSTRACT

Data transaksi penjualan merupakan sebuah data yang berisi beberapa data peribadi seperti nama customer, alamat customer, nomor handphone customer, dan lain-lain yang bersifat rahasia. Kebanyakan data transaksi penjualan hanya disimpan begitu saja tanpa ada kemanan yang bisa mengamankan data-data tersebut dari pihak yang tidak seharusnya tau data-data tersebut.

Dari uraian diatas perlu suatu sistem yang dapat membantu mengatasi permasalahan tersebut, yaitu dengan membangun sebuah sistem dengan penerapan kriptografi untuk mengamankan data transaksi penjualan pada PT. MITSUBISHI ELECTRIC INDONESIA menggunakan algoritma Advanced Encryption Standard (AES) 128 bit, dengan dibangunnya sistem ini diharapkan dapat membantu pihak PT. MITSUBISHI ELECTRIC INDONESIA dalam mengatasi permasalahan yang terjadi

Hasil penelitian merupakan terciptanya sebuah aplikasi pengamanan data dengan Algoritma Advanced Encryption Standard (AES) 128 bit yang dapat membantu admin dalam mengamankan data transaksi penjualan di PT. MITSUBISHI ELECTRIC INDONESIA.

Copyright © 2019 STMIK Triguna Dharma.
All rights reserved

First Author
Nama : Fandi Ahmad Sitorus
Kampus : STMIK Triguna Dharma
Program Studi : Sistem Informasi
E-Mail : fandiahmad1782@gmail.com

1. PENDAHULUAN

PT. MITSUBISHI ELECTRIK adalah perusahaan multinational asal Jepang yang memproduksi peralatan listrik dan elektronik. Perusahaan ini berpusat di Tokyo, pertama kali didirikan pada tahun 1921 dan mempunyai kantor di seluruh dunia salah satunya di indonesia tepatnya di Kota Medan, Mitsubishi Electric adalah salah satu nama terkemuka di dunia dalam manufaktur penjualan produk dan sistem kelistrikan elektronik yang di gunakan berbagai bidang dan aplikasi.

Saat ini perusahaan tersebut memiliki banyak data-data rahasia dan pesan rahasia seperti data diri, data transksi penjualan, dan data-data rahasia lainnya yang dimana data-data tersebut bersifat privasi. Sehubung dengan penelitian ini saya mengambil kesempatan untuk membantu perusahaan tersebut dalam mengamankan data-data bersifat privasi yang mereka miliki.

Kriptografi merupakan keahlian atau ilmu dalam menyandikan atau mengamankan sebuah data atau informasi seperti integritas data, kerahasiaan data, autentikasi data, dan data-data yang bersifat privasi lainnya, agar tidak dapat diketahui oleh pihak yang tidak berhak pada data atau informasi tersebut. Kriptografi sendiri merupakan seni untuk mengamankan data yang didalamnya terdapat algoritma tertentu yang bertujuan sebagai *confusion* atau pengacakan, dengan cara mengubah teks asli (*plaintext*) menjadi teks yang tidak bisa dibaca secara langsung oleh manusia atau teks rahasia (*ciphertext*). Kriptografi mempunyai proses enkripsi dimana dapat mengubah teks atau data (*plaintext*) menjadi teks rahasia (*ciphertext*), kemudian sebaliknya proses deskripsi yang dapat mengembalikan teks rahasia (*ciphertext*) menjadi teks atau data *(plaintext*).

Dalam proses ini digunakan kunci rahasia, semakin banyak kunci rahasia yang digunakan maka semakin bagus. kriptogrfi dapat dibedakan menjadi dua macam yaitu simetrik dan asimetrik. Algoritma simetrik (model enkripsi konvensional) merupakan algoritma yang menggunakan satu kunci untuk proses enkripsi dan deskripsi data. Sedangkan algoritma asimetrik (model enkripsi kunci publik) menggunakan kunci yang berbeda dalam proses enkripsi dan deskripsi pesan[1].

Adapun algoritma yang digunakan pada penelitian ini yaitu algoritma *Advanced Encryption Standard* (AES) adalah sebuah algoritma kriptografi yang digunakan untuk mengamankan sebuah data atau informasi. Algoritma AES merupakan standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) yang digunakan sebagai pengganti algoritma DES *(Data Encryption Standard)* yang sudah berakhir masa penggunaanya pada tahun 2001[2].

Berdasarkan latar belakang permasalahan diatas, maka diangkat sebuah penelitian dengan judul **"Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit Untuk Keamanan Data Transaksi Penjualan Pada PT. MITSUBISHI ELECTRIC INDONESIA"**

2. KAJIAN PUSTAKA

2.1 Kriptografi

Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data**.** Kriptografi merupakan ilmu dan seni untuk nenjaga kerahasiaan dari suatu pesan dengan cara mengubah pesan tersebut kedalam bentuk yang tidak lagi dimengerti maknanya[3].

2.2 Algoritma *Advanced Encryption Standard* (AES) 128 Bit

Advanced Encryption Standard adalah algoritma kriptografi simetris yang dapat digunakan untuk mengamankan sebuah data informasi. Algoritma ini merupakan standar enkripsi dengan kunci simetris. Beberapa mode operasi yang dapat diterapkan pada algoritma kriptografi penyandi blok AES di antaranya adalah *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), dan *Output Feedback* (OFB). Implementasi AES dengan mode operasi ECB, CBC, CFB, dan OFB tentu saja memiliki kelebihan dan kekurangan tertentu dalam aspek tingkat keamanan data. Algoritma kriptografi bernama *Rijndael* yang didesain oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes. Algoritma kriptografi pengganti DES yang diadakan oleh NIST *(National Institutes of Standards and Technology)* milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma *Rijndael* inilah yang kemudian dikenal dengan *Advanced Encryption Standard* (AES). Setelah mengalami beberapa proses standardisasi oleh NIST, *Rijndael* kemudian diadopsi menjadi *standard* algoritma kriptografi secara resmi pada

22 Mei 2002. Pada 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetris[4]

2.3 Proses Ekspansi

Proses ekspansi kunci Algoritma *Advanced Encryption Standard* mengambil kunci cipher dan melakukan ekspansi kunci untuk membentuk *key schedule.* Ekspansi kunci akan menghasilkan total Nb (Nr+1) *word*. Agar *Advanced Encryption Standard* 128 bit dapat digunakan maka 4(10+1) = 40 *word* = 44 x 32 bit = 1408-bit *subkey*. Ekspansi kunci dari 128 menjadi 1408-bit *subkey*. Proses ini lah disebut dengan *key schedule*. *Subkey* diperlukan karena setiap *round* merupakan suatu nilai inisial dari Nb *word* untuk 11 Nr = 0 dan 2 untuk Nr = 1,3 untuk Nr = 2…., yang berisi *array linier* empat *byte* word (w), 0=1 Nb (Nr + 1).

2.3.1 Proses Enkripsi

Enkripsi yaitu melakukan proses pengubahan pesan atau penyandian data dari pesan asli (*plaintext*) di konversi menjadi bentuk yang tidak jelas untuk dipahami bahkan dimengerti. Algoritma *advanced encryption standard* memiliki panjang kunci 128-bit yang terdiri dari *AddRoundKey*, *SubBytes*, *ShiftRows* dan *MixColumms*[5].

2.3.2 Proses Dekripsi

Dekripsi merupakan suatu proses pengembalian data ke bentuk semula yang telah terenkripsi (*chipertext*) dan dapat di baca kembali seperti *plaintext*. Transformasi pada dekripsi sama dengan proses pada transformasi enkripsi. Namun, pada transformasi *chipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma *advanced enryption standard*. Transformasi *byte* yang digunakan pada *invers cipher* adalah *InvShiftRows, InvSubBytes, InvMixColumns,* dan *AddRoundKey*[6]

3. METODE PENELITIAN

3.1 Metodologi Penelitian

Metode penelitian merupakan suatu hal yang sangat penting dalam melakukan sebuah penelitian, metode penelitian adalah cara sistematis untuk memecahkan sebuah masalah penelitian dan dapat dipahami sebagai ilmu yang mempelajari bagaimana penelitian dilakukan secara ilmiah.

Dalam teknik pengumpulan data dilakukan dengan dua tahapan,
diantaranya yaitu:

1. Observasi

   Dalam penelitian ini dilakukan observasi pra-riset telebih dahulu untuk mencari masalah yang terjadi di PT. MITSUBISHI ELECTRIC INDONESIA cabang medan terkhusus dalam pengamanan data transaksi penjualan, dari masalah tersebut masalah akan dirumusakan dalam penelitian ini sehingga dapat menemukan rumusan apa saja yang perlu dipersiapkan untuk bagaimana cara menyelesaikan masalah tersebut.

2. Wawancara

   Tujuan dari wawancara untuk mencari suatu informasi atau data yang dibutuhkan seorang peneliti dengan cara tanya jawab kepada yang ditanyakan. Dalam hal ini proses wawancara berlangsung dengan pihak perusahaan yang berwenang untuk mengakses data transaksi penjualan pada PT. MITSUBISHI ELECTRIC INDONESIA

   Berikut adalah data yang di dapatkan dari PT. MITSUBISHI ELECTRIC INDONESIA :

Tabel 3.1 Sampel Data transaksi penjualan di PT. MITSUBISHI ELECTRIC INDONESIA

No	Serial Nomor	Nama *Customer*	Nama Kasir	Alamat *Customer*	No Hp *Customer*	Tanggal Pembelian
1.	W21317 Y0998	DESTRI AYUNI SRG	LENNI	Jln. Karya Kasih Gg. Kasih 10	0823552583 21	11/12/2018
2.	W12018 70687	WAHYUDI PRASETYO	LENNI	Jln. Medan Binjai Km 12,5 no 102	0812648996 21	13/12/2018
3.	W12117 70434	JANUAR RAMADHANA	LENNI	JL.PINTU AIR 4 NO.92	0852769249 25	14/12/2018
4.	W21318 21025	WARDANA SIMAMORA	ERNA	JL.INTAN NO.22B MEDAN AREA SEI RENGAS II	0821602321 22	15/12/2018

3.2 Metode Perancangan Sistem

Di dalam penelitian ini, dijadikan sebuah metode peracangan sistem yaitu *waterfall algoritm.* Berikut ini adalah fase yang dilakukan dalam penelitian yaitu:
Analisis masalah dan kebutuhan desain sistem, pembangunan sistem, dan implementasi sistem

3.2.1 Penyelesaian

Berikut ini adalah data transksi penjualan yang di dapat dari PT. MITSUBISHI ELECTRIC INDONESIA yang akan diamankan. Dalam pengujiannya, sebagai contoh data yang digunakan sebagai sampel dalam penelitian ini yaitu sebagai berikut:

Tabel 3.2 Sampel Data transaksi penjualan di PT. MITSUBISHI ELECTRIC

No	Serial Nomor	Nama *Customer*	Nama Kasir	Alamat *Customer*	No Hp *Customer*	Tanggal Pembelian
1.	W21317 Y0998	DESTRI AYUNI SRG	LENNI	Jln. Karya Kasih Gg. Kasih 10	082355258321	11/12/2018

3.3.3 Penyelesaian Masalah Dengan Menggunakan Algortima AES 128 bit

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

3.3.3.1 Proses Enkripsi algoritma AES 128 bit

Proses enkripsi algoritma AES, ada dua tahapan yaitu proses ekspansi kunci dan proses enkripsi sebagai berikut:

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 "fandiahmadsitoru".
   a. Urutkan kunci kedalam blok berukuran 128 bit (16 kode ASCII). Lalu ubah kunci kedalam bentuk heksadesimal

f	a	n	d	i	a	h	m	a	d	s	i	t	o	r	u
66	61	6E	64	69	61	68	6D	61	64	73	69	74	6F	72	75

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

66	69	61	74
61	61	64	6F
6E	68	73	72
64	6D	69	75

   State diatas merupakan cipherkey/kunci ronde ke-0

   c. Setelah itu, untuk mendapatkan kolom pertama hingga ke sepuluh, langkah selanjutnya yaitu dilakukan fungsi *RotWord, SubByte,* dan XOR antara kolom pertama dari kunci ronde ke-0, hasil dari *SubBytes* lalu di-XOR-kan lagi dengan *RCon*, sehingga mendapatkan hasil ronde ke-10 sebagai berikut:

69	4F	9A	90
D4	19	DD	43
1D	B6	A6	9C
A5	93	45	B2

2. Proses Enkripsi
   Plaintext yang akan digunakan yaitu "DESTRI AYUNI SRG". Kemudian urutkan kedalam blok lalu ubah kedalam bilangan heksadesimal.

D	E	S	T	R	I		A	Y	U	N	I		S	R	G
44	45	53	54	52	49	20	41	59	55	4E	49	20	53	52	47

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

44	52	59	20
45	49	55	53
53	20	4E	52
54	41	49	47

Lakukan XOR antara *plainteks* dengan *RoundKey* 0. Proses ini dinamakan *AddRoundKey*.

44	52	59	20	XOR	66	69	61	74	=	22	3B	38	54
45	49	55	53		61	61	64	6F		24	28	31	3C
53	20	4E	52		6E	68	73	72		3D	48	3D	20
54	41	49	47		64	6D	69	75		30	2C	20	32

Proses *AddRoundKey* diatas masih sebagai *pra-round* dan akan menjadi masukan untuk ronde ke1 yang akan diproses dengan 4 transformasi yaitu *SubBytes*, *ShiftRows*, *MixColumns* dan *AddRoundKey*.

a. Hasil dari *pra-round* disubtitusikan dengan nilai pada tabel *S-Box* (*SubBytes*).

22	3B	38	54
24	28	31	3C
3D	48	3D	20
30	2C	20	32

→

93	E2	07	20
36	34	C7	EB
27	52	27	B7
04	71	B7	23

b. Lakukan *ShiftRows* pada hasil dari 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.

93	E2	07	20
36	34	C7	EB
27	52	27	B7
04	71	B7	23

→

93	E2	07	20
34	C7	EB	36
27	B7	27	52
23	04	71	B7

c. Transformasi *MixColumns* dengan mengoperasikan *state* kolom demi kolom pada *state* kolom, dengan mengkoversikan setiap kolom sebagai polinomial.

93	E2	07	20
34	C7	EB	36
27	B7	27	52
23	04	71	B7

x

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \end{pmatrix}$$

=

65	3E	7E	FF
B1	B1	D2	0D
8C	5C	31	70
FB	45	27	71

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

MixColumns					*RoundKey* Ke-1					*AddRoundKey*			
65	3E	7E	FF	XOR	CF	A6	C7	B3	=	AA	98	B9	4C
B1	B1	D2	0D		21	40	24	48		90	F1	F6	46
8C	5C	31	70		F3	9B	E8	9A		7F	C7	D9	EA
FB	45	27	71		F6	9B	F2	87		0D	DE	D5	F6

e. Lakukan proses diatas sampai 10 kali putaran (*round*) Hingga mendapatkan putaran ke-10. Berikut adalah hasil enkripsi hingga *round* ke 10:

76	80	AC	D2
B0	EB	9C	40
0F	E1	0D	EF
FC	64	5D	36

Hasil dari proses *AddRoundKey* atau *round* ke-10 diubah ke bentuk karakter didalam tabel ASCII.

Tabel 3.3 Tabel *Round*, Kode ASCII dan Karakter untuk *Cipherteks*

Round	**Kode ASCII**	**Karakter**
76	118	V
B0	176	▒
0F	15	**SI**
FC	252	³
80	128	Ç
EB	235	Ù
E1	225	ß
64	100	D
AC	172	¼
9C	156	£
0D	13	**CR**
05	5	**ENQ**
D2	210	Ê
40	64	@
EF	239	´
36	54	6

Dan hasil dari enkripsi dengan algoritma AES menghasilkan cipherteks sebagai berikut.

Tabel 3.4 Hasil Enkripsi Dengan Algoritma AES

No	Serial Nomor	Nama *Customer*	Nama Kasir	Alamat *Customer*	No Hp *Customer*	Tanggal Pembelian
1.	W2131 7Y0998	v▒SI³ÇÙ ßd¼£CR ENQÊ@´6	LENNI	Jln. Karya Kasih Gg. Kasih 10	0823552583 21	11/12/2018

3.3.3.2 Proses Dekripsi algoritma AES 128 bit

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.

v	▒	**SI**	³	Ç	Ù	ß	d	¼	£	**CR**	**ENQ**	Ê	@	´	6
76	B0	0F	FC	80	EB	E1	64	AC	9C	0D	5D	D2	40	EF	36

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

76	80	AC	D2
B0	EB	9C	40
0F	E1	0D	EF
FC	64	5D	36

Lakukan XOR antara *cipherteks* dengan *RoundKey* Ke-10. Proses ini dinamakan *AddInvRoundKey*.

IF	CF	36	42
64	F2	41	03
12	57	A5	73
59	F7	18	84

XOR

69	4F	9A	90
D4	19	DD	43
1D	B6	A6	9C
A5	93	45	B2

=

IF	CF	36	42
64	F2	41	03
12	57	A5	73
59	F7	18	84

Proses *AddInvRoundKey* diatas masih dalam *initial-round*, dan akan menjadi masukan untuk ronde ke-1 yang akan diproses dengan 4 transformasi yaitu *InvShiftRows*, *InvSubBytes*, *AddInvRoundKey*, dan *InvMixColumns*.

1. Lakukan *InvShiftRows* pada hasil *initial-round* dari *AddInvRoundKey* yang dieksekusi lewat pergeseran *siklik* secara memutar. Baris ke dua digeser secara *siklik* ke kiri tiga kali, baris ke tiga dua kali, baris ke empat sekali.

IF	CF	36	42
64	F2	41	03
12	57	A5	73
59	F7	18	84

IF	CF	36	42
03	64	F2	41
A5	73	12	57
F7	18	84	59

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

IF	CF	36	42
03	64	F2	41
A5	73	12	57
F7	18	84	59

→

CB	5F	24	F6
D5	8C	04	F8
29	8F	39	DA
26	34	4F	15

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

CB	5F	24	F6
D5	8C	04	F8
29	8F	39	DA
26	34	4F	15

XOR

54	26	D5	0A
CC	CD	C4	9E
75	1E	1E	34
C2	D6	D6	F7

=

9F	79	F1	FC
19	41	C0	66
5C	24	29	EE
E4	02	99	E2

4. Hasil *AddInvRoundKey* ditransformasikan oleh *InvMixColumns* dengan mengoperasikan setiap *state* kolom. Operasi ini dilakukan pada *state* kolom dengan mengkoversikan setiap kolom sebagai polinomial.

9F	79	F1	FC
19	41	C0	66
5C	24	29	EE
E4	02	99	E2

X

$$\begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \end{pmatrix}$$

=

04	88	16	38
41	0A	96	7B
64	85	36	0B
E7	0D	53	1E

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

44	52	59	20
45	49	55	53
53	20	4E	52
54	41	49	47

Hasil dari proses *AddRoundKey* atau *round* ke-10 ubah ke bentuk karakter didalam tabel ASCII. Sebagai berikut:

Tabel 3.5 Tabel *Round,* Kode ASCII dan Karakter untuk *Plainteks*

Round	**Kode ASCII**	**Karakter**
44	68	D
45	69	E
53	83	S
54	84	T
52	82	R
49	73	I
20	32	
41	65	A
59	89	Y
55	85	U
4E	78	N
49	73	I
20	32	
53	83	S
52	82	R
47	71	G

Dan hasil dari dekripsi dengan algoritma AES menghasilkan plainteks sebagai berikut.

Tabel 3.6 Hasil Dekripsi Dengan Algoritma AES

No	**Serial Nomor**	**Nama *Customer***	**Nama Kasir**	**Alamat *Customer***	**No Hp *Customer***	**Tanggal Pembelian**
1.	W2131 7Y0998	DESTRI AYUNI SRG	LENNI	Jln. Karya Kasih Gg. Kasih 10	0823552583 21	11/12/2018

IMPLEMENTASI DAN PENGUJIAN

1. Form login

   Form login merupakan tampilan ketika pengguna menjalankan program. Tampilan ini berisikan *username* dan *password* yang harus di isi terlebih dahulu

Gambar 4.12 *form* login

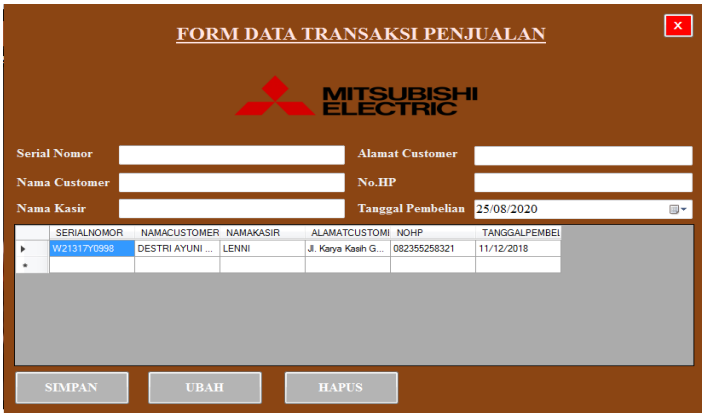
2. Form menu utama

   Merupakan tampilan awal pada saat aplikasi dijalankan

Gambar 4.13 form menu utama

3. Form data transaksi penjualan

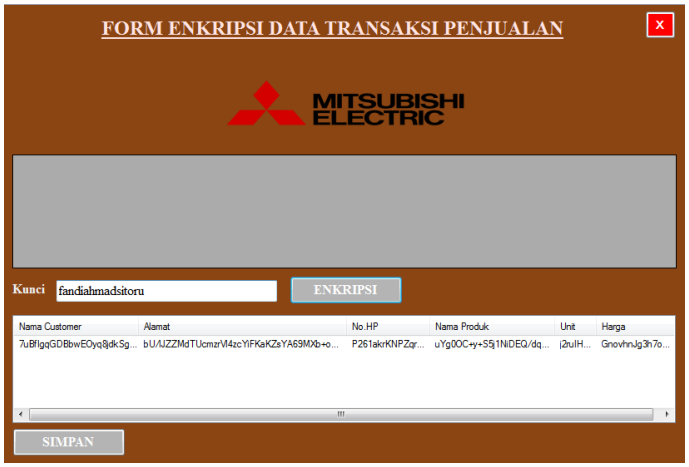
   Form ini berfungsi untuk mengolah data transaksi penjualan pada PT. MITSUBISHI ELECTRIC INDONESIA



Gambar 4.14 *form* input data transaksi penjualan

4. Form enkripsi

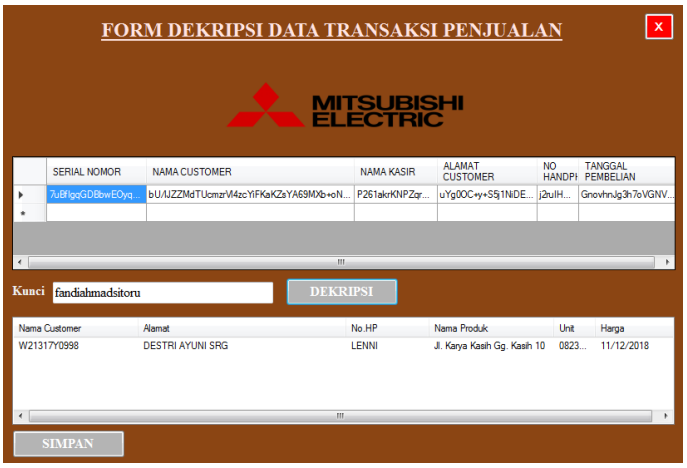
Form ini berfungsi untuk enkripsi data transaksi penjualan



Gambar 4.15 *form* enkripsi

5. Form dekripsi

Form ini berfungsi untuk dekripsi data transaksi penjualan



Gambar 4.16 *form* dekripsi

5.1 KESIMPULAN

Berdasarkan penelitian yang telah dilalui dalam tahap perancangan dan evaluasi kriptografi dalam mengamankan data transaksi penjualan pada PT. MITSUBISHI ELECTRIC INDONESIA menggunakan metode *Advanced Encryption Standard* 128 bit maka dapat disimpulkan bahwa:

1. Untuk mengamankan data transaksi penjualan yang bersifat rahasia akan diamankan menggunakan algoritma kriptografi *Advanced Encryption Standard* 128 bit.
2. Algoritma *Advanced Encryption Standard* 128 bit 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 dan dapat mengoptimalkan dalam pengamanan data untuk mengamankan data.
3. Dengan cara merancang sistem aplikasi yang dapat digunakan dalam mengamankan data 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* 128 bit, sehingga sistem ini mampu membantu admin dalam mengamankan data.

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 *admin* 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 kepada PT. MITSUBISHI ELECTRIC INDONESIA, disarankan agar sistem ini juga dapat di gunakan untuk perusahaan lainnya.
4. Diharapkan dalam penelitian selanjutnya dapat membangun Sistem Pengamanan Data dengan menggunakan algoritma dan aplikasi yang lain.

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 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 mahasiswa dalam isi dan tata bahasa selama menyelesaikan skripsi.
5. Ibu Usti Fatimah Sari Sitorus Pane , S.Kom, M.Kom selaku Dosen Pembimbing II yang membimbing mahasiswa dalam teknik penulisan skripsi.
6. Seluruh Dosen, Staff dan Pegawai STMIK Triguna Dharma.
7. Terimakasi juga disampaikan kepada PT. MITSUBISHI ELECTRIC INDONESIA 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] G. W. Bhaudhayana and I. M. Widiartha, "Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap," *J. iImu Komput. Univ. Udayana*, vol. 8, no. 2, pp. 15–25, 2015.

[2] A. Kusyanti and K. Amron, "Analisis Perbandingan Algoritma Advanced Encryption Standard Untuk Enkripsi Short Message Service (SMS) Pada Android," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 10, pp. 4281–4289, 2018.

[3] R. Tullah, M. I. Dzulhaq, and Y. Setiawan, "Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard (AES)," *J. Sisfotek Glob.*, vol. 6, no. 2, pp. 24–30, 2016.

[4] J. Prayudha, "Implementasi Keamanan Data Gaji Karyawan Pada PT . Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *Sains dan Komput.*, vol. 18, no. 2, 2019.

[5] V. Novianty, J. Algoritma, S. Tinggi, T. Garut, and I. Pendahuluan, "Mengamankan Basis Data Keuangan Koperasi," *J. Algoritm. Sekol. Tinggi Teknol. Garut*, vol. Vol. 12, pp. 1–7, 2015.

[6] G. Gumira, Ernawati, and A. Erlanshari, "Implementasi Metode Advanced Encryption Standard (AES) Dan Message Digest 5 (MD5) Pada Enkripsi Dokumen (Studi Kasus LPSE UNIB)," *J. Rekursif*, vol. 4, no. 3, pp. 277–287, 2016.

BIOGRAFI PENULIS

<table>
<tr>
<td>  </td>
<td>Data Diri

Nama : Fandi Ahmad Sitorus
Tempat/Tanggal Lahir : Medan, 11 Juli 1998
Jenis Kelamin : Laki Laki
Agama : Islam
Status : Belum Menikah
Pendidikan Terakhir : Sekolah Menengah Kejuruan
Kewarganegaraan : Indonesia
E-mail : fandiahmad1782@gmail.com

Pendidikan Formal

1. Tahun 2004 - 2010 : SD 067952
2. Tahun 2010 -2013 : SMP Swasta Pembangun
3. Tahun 2013 -2016 : SMK Multi Karya</td>
</tr>
<tr>
<td>  </td>
<td>Nurcahyo Budi Nugroho, S.Kom., M.Kom
NIDN : 0130038201
E-mail : nurcahyobn@gmail.com
Dosen pengajar tetap STMIK TRIGUNA DHARMA</td>
</tr>
<tr>
<td>  </td>
<td>Usti Fatimah Sari Sitorus Pane, S.Kom., M.Kom
NIDN : 0120089101
E-mail : ustipaneee@gmail.com
Dosen pengajar tetap STMIK TRIGUNA DHARMA</td>
</tr>
</table>