Jurnal CyberTech

Vol.x. No.x, September 201x, pp. xx~xx
P-ISSN : 9800-3456
E-ISSN : 2675-9802

IMPLEMENTASI KRIPTOGRAFI UNTUK MENGAMANGKAN DATA PENJUALANAN DI PT. PAPPARICH MEDAN MENGGUNAKAN METODE AES 128

Dian Pratomo[*],Nurcahyo Budi Nugroho [**], Rico Imanta Ginting[**]

* Program Studi Sistem Informasi, STMIK Triguna Dharma
** Program Studi Tehnik Komputer, STMIK Triguna Dharma

Article Info

Article history:
Received Jun 12th, 201x
Revised Aug 20th, 201x
Accepted Aug 26th, 201x

Keyword:
AES
Penyandian File
Algoritma Kunci Simetris

ABSTRACT

Advanced Encryption Standard (AES) adalah sebuah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Dalam algoritma kriptografi AES 128, 1 blok plaintext berukuran 128 bit terlebih dahulu di konversikan menjadi matriks heksadesimal berukuran 4x4 yang disebut state. Setiap elemen state berukuran 1 byte. Proses enkripsi pada AES merupakan transformasi terhadap state secara berulang dalam 10 ronde. Setiap ronde AES membutuhkan suatu kunci hasil dari generasi kunci yang menggunakan 2 transformasi yaitu subtitusi dan tranformasi. Pada proses enkripsi AES menggunakan 4 tranformasi dasar dengan urutan transformasi subbyte, shiftrows, mixcoloums, dan addroundkey. Sedangkan pada proses dekripsi menggunakan semua invers transformasi dasar pada algoritma AES kecuali addroundkey dengan urutan transformasi invshiftrows, invsubytes, addroundkey dan invmixcoloums. Pada data teks, proses enkripsi diawali dengan mengkonversikan teks mejadi kode ASCII dalam bilangan heksadesimal yang dibentuk menjadi matriks byte 4x4. Selanjutnya dilakukan beberapa transformasi dasar seperti subbyte, shiftrows, mixcolumns, dan addroundkey.Kriptografi AES 128 bit memiliki ruang kunci yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan sehingga terhindar dari brute force attack.

Kata Kunci: AES, Penyandian file, Algoritma kunci simetris.

Corresponding Author: *First Author
Nama :Dian Pratomo
Program Studi : Sistem Informasi
STMIK Triguna Dharma
Email:ddsdianpratomo1407@gmail.com

1. PENDAHULUAN

Di Indonesia sendiri perkembangan bisnis kuliner juga berkembang pesat dimana beberapa tahun belakangan ini banyak menjamur restoran asing maupun local, seperti restoran cepat saji ,restoran cina, restoran western dengan brand local yang memiliki cir khas masing-masing baik yang berdiri sendiri maupun dalam lingkup hotel/mall. PT. Papparich sendiri hadir pertama kali di Indonesia tepatnya di Plaza Medan Fair Medan, Sumatera utara pada tanggal 10 april 2016, sampai saat ini Papparich hanya hadir di dua kota besar di Indonesia yaitu Medan dan Kota Jakarta, di perlukan strategi pemasaran yang baik dalam mempertahankan eksistensi suatu merek tersebut[2]. Keamanan informasi merupakan hal yang paling penting yang tidak boleh bocor ke public atau segelintir orang, jika informasi bocor maka akan merugikan bagi penerima dan pengirim informasi[3]. Maka karenanya untuk itu diperlukan pengoptimalan keamanan data dengan menggunakan kriptografi AES (*Advanced Encryption Standard*).

2. TINJAUAN PUSTAKA

2.1 Kriptografi (*Security System*)

Kriptografi adalah ilmu dan seni untu k menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain, *Advanced Encryption Standard* (AES) merupakan algoritma kriptografi yang dapat digunakan untuk mengamankan data, Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) [4]. Kriptografi adalah ilmu yang mempelajari tahnik-tehnik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, intregitas data, otentikasi dan anti penyangkalan. Kroptografi dapat diartikan sebagai ilmu untuk menjaga kerahasiaan informasi dengan metode dan tehnik yang mencakup *Confidentialiti, intregitas, authentication*[6].

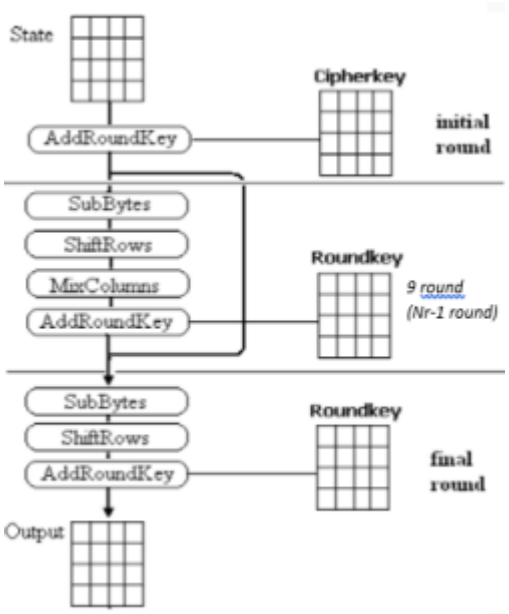
2.2 AES (*Advanced Encryption Standard*)

Pada November 2001 *National Institute of Standard and Technology* (NIST) mensosialisasikan sebuah standard baru enkripsi yang dikembangkan dengan algoritma DES (*Data Encryption Standard*) melalui seleksi ketat dengan algoritma lainnya dan diberi nama Algoritma *Advanced Encryption Standard* (AES) atau algoritma Rijindael. Algoritma ini dicetuskan oleh Vincent Rijmen dan Jian Daemen yang menjadi pemenang saat lomba seleksi algoritma baru pengganti DES, “alas an utama terpilihnya algoritma ini memiliki keseimbangan antara kemanan serta fleksibilitas dalam berbagai platform softwere dan hardwere”[9].

2.3 Algoritma Metode *AES (Advanced Encryption Standard)*

Adapun algoritma dari penyelesaian dari metode *AES* yaitu sebagai berikut:

Algoritma AES mengambil kunci cipher dan melakukan rutin ekspansi kunci (key expansion) untuk membentuk key schedule. Ekspansi kunci menghasilkan total Nb(Nr+1) word. Algoritma ini membutuhkan set awal key yang terdiri dari Nb word, dan setiap round Nr membutuhkan data kunci sebanyak Nb word. Hasil key schedule terdiri dari array 4 byte word linear yang dinotasikan dengan [wi]. SubWord adalah fungsi yang mengambil 4 byte word input dan mengaplikasikan S-Box ke tiap-tiap data 4 byte untuk menghasilkan word output. Fungsi RotWord mengambil word [a0, a1, a2, a3] sebagai input, melakukan permutasi siklik, dan mengembalikan word [a1, a2, a3, a0]. Rcon[i] terdiri dari nilai-nilai yang diberikan oleh [xi-1, {00}, {00}, {00}], dengan xi-1 sebagai pangkat dari x (x dinotasikan sebagai {02}).



Gambar 2.1 Menjelaskan tentang proses Enkripsi AES 128

3. METODE PENELITIAN

Metode penelitian langkah yang dimiliki dan dilakukan oleh peneliti dalam rangka untuk mengumpulkan informasi atau data serta melakukan investigasi pada data yang telah didapatkan tersebut. Metode penelitian memberikan gambaran rancangan penelitian yang meliputi antara lain: prosedur dan langkah-langkah yang harus ditempuh, waktu penelitian, sumber data, dan dengan langkah apa data-data tersebut diperoleh dan selanjutnya diolah dan dianalisis.

Tabel 1 Data Penjualanan

NO	Periode	Admin	Menu	Jumlah Penjulanan	Harga	Pendapatan
1	01/01/20	Sherinta Cash	Nasi Briyani Beef Rendang	150	Rp. 45.000	Rp. 6.750.000
2	01/02/20	Sherinta Cash	Fried Chicken Thigh	219	Rp. 76.000	Rp. 16.644.000
3	01/03/20	Sherinta Cash	Nasi Lemak	300	Rp. 50.000	Rp. 15.000.000
4	01/04/20	Dwi Andini	PappaChicken Rice Set	250	Rp. 45.000	Rp. 11.250.000
5	01/05/20	Dwi Andini	Pappa Curry Laksa	259	Rp. 67.000	Rp. 17.353.000
6	01/06/20	Angel Melati	Ipoh Kway Teow Soup	100	Rp. 35.000	Rp. 3.500.000
7	01/07/20	Lusiana	Seafoof Char Kway teow	179	Rp. 40.000	Rp. 7.160.000
8	01/08/20	Lusiana	Pappa Fried mee	230	Rp. 60.000	Rp. 13.800.000
9	01/09/20	Chih ming	Pappa Bun	200	Rp. 60.000	Rp. 12.000.000
10	01/10/20	Usman	Pappa Canai With chicken	400	Rp. 30.000	Rp. 12.000.000
				Total Pendapatan Di Tahun 2020		Rp. 115.457.000

3.1 Metode pengembangan Sistem

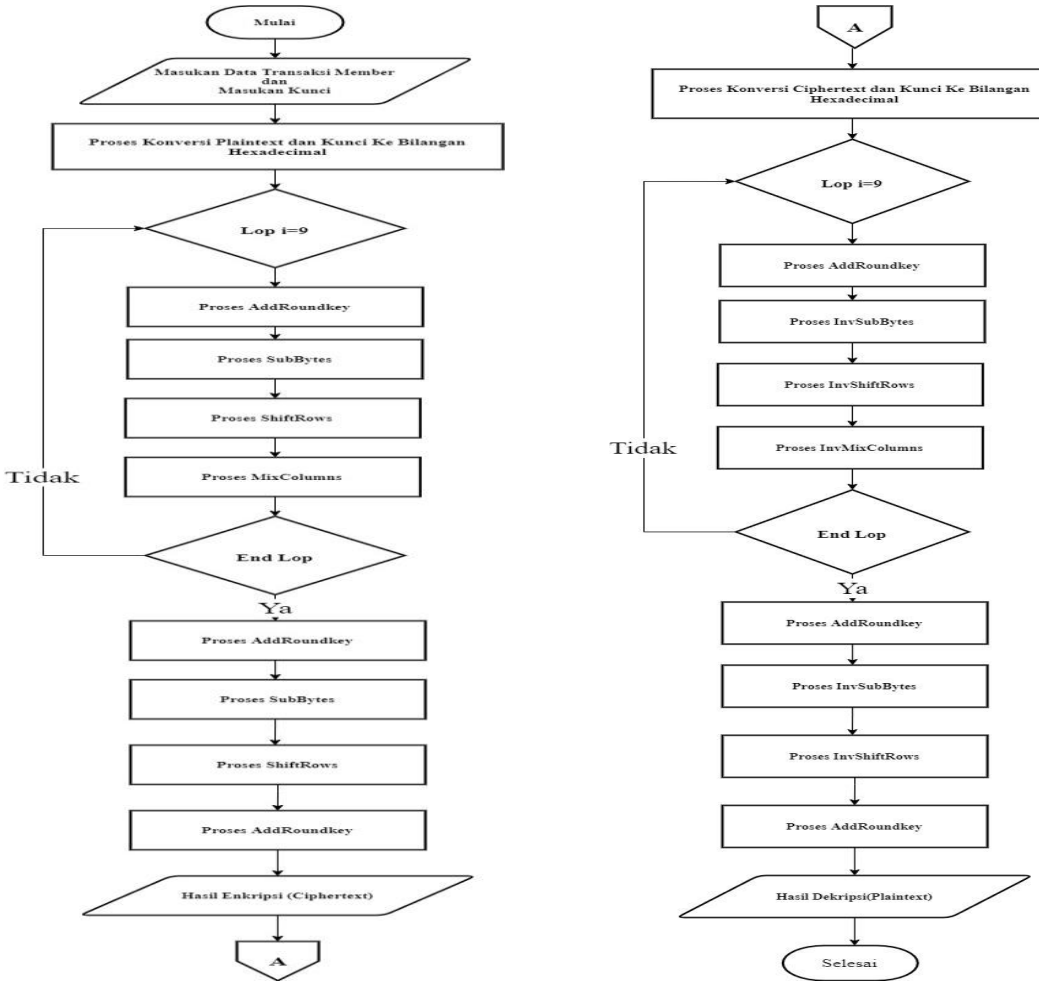
Di dalam penelitian ini di gunakan sebuah metode perancangan sistem yaitu model linier (*Waterfall*) dalam menyelesaikan suatu permasalahan dalam sebuah sistem tersebut.

3.2 Algoritma Sistem

Algoritma sistem merupakan salah satu urutan maupun langkah-langkah cara pembuatan sistem sehingga memberikan intruksi atau sebuah perintah keluaran yang diinginkan berdasarkan ide atau masukan yang diberikan.

3.2.1 Flowchart Sistem

Flowchart sistem merupakan bagan yang menunjukan alur kerja atau apa yang sedang dikerjakan didalam sistem secara keseluruhan dan menjelaskan urutan dari prosedur-prosedur yang ada didalam sistem. Berikut ini adalah *flowchart* sistem Enkripsi dan Dekripsi.



Gambar 2.2 *Flowchart* sistem Enkripsi dan Dekripsi

1. Adapun proses penyelesaian enkripsi dan dekripsi dari data yang akan diamankan adalah sebagai berikut:
   a. Perhitungan Enkripsi
      Plaintext : Sherinta Cash
      Plaintext dalam hexadecimal (128 bits) : 53 68 72 69 6E 74 61 20 14 43 61 73 68 14 14 14
      Key : PAPPARICHSUNYAYA
      Plaintext dalam hexadecimal (128 bits) : 50 41 50 50 41 52 49 43 48 53 55 4E 59 41 49 41
   b. Mencari nilai Wi-1Wi

41	83
59	CB
41	83
59	CB

SubBytes

50	83	01	D2
41	CB	00	8A
50	83	00	D3
50	CB	00	9B

Adapun perhitungan secara manualnya yaitu sebagai berikut:
50 (Hex) = 01010000
83 (Hex) = 10000011
01 (Hex) = 00000001
Hasil = 11010010 (Bin) = D2 (Hex)

Chiper Key				Wi-1Wi Round 1				Wi-2Wi Round 2			
50	41	48	59	D2	93	DB	82	A4	37	EC	6E
41	52	53	41	8A	D8	8B	CA	1A	C2	49	83
50	49	55	59	D3	9A	CF	96	DD	47	88	1E
50	43	4E	41	9B	D8	96	D7	88	50	C6	11

Wi-10 Wi Round 10			
45	18	FF	F2
6	6	A3	9F
54	43	27	ED
D5	0C	DB	87

2. Langkah kedua yang haru dilakukan yaitu melakukan xor antara plaintetxt dan kunci, seperti berikut:

03	28	5C	31	XOR	50	41	48	59	=	53	69	14	68
29	3C	10	55		41	52	53	41		68	6E	43	14
35	3D	34	4D		50	49	55	59		65	74	61	14
22	22	3D	55		50	43	4E	41		72	61	73	14

a. Hasil Proses *Subbyte* (menggunakan table s-box)

ED	F9	FA	45
45	9F	1A	FA
4D	92	EF	FA
40	EF	8F	FA

b. Transformasi *ShiftRows*

ED	F9	FA	45
9F	1A	FA	45
EF	FA	4D	92
FA	40	EF	8F

c. Proses *Mix Columns*

ED	F9	FA	45
9F	1A	FA	45
EF	FA	4D	92
FA	40	EF	8F

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} ED \\ 9F \\ EF \\ FA \end{bmatrix}$$

Hasil dari *Mix Columns*

74	7D	2D	2D
1D	8D	4D	9F
9F	CC	1A	39
AE	61	B4	F1

3. Pada ronde pertama didapat Chipertext yang akan menjadi masukan atau input untuk ronde 2, begitu juga cipertext yang didapat pada ronde 2 kan digunakan menjadi input pada ronde 3. Proses seperti ini berlangsung hingga ronde 10. Pada ronde 10 didapat nilai enkripsi sebagai berikut:

Ronde 10 :

Sub byte =

B1	E0	E3	C9
69	62	60	42
6A	01	A6	4E
5E	30	FE	0A

ShiftRows =

B1	E0	E3	C9
62	60	42	69
A6	4E	6A	01
0A	5E	30	FE

AddroundKey =

F4	F8	1C	3B
64	66	E1	F6
F2	0D	4D	EC
DF	52	EB	79

4. Pada ronde ke 10 transformasi yang dilakukan hanya 3 yaitu, *Subbyte, Shiftrows, AddroundKey*. Dan diddapat cipertext sebagai berikut:

Chipertext =

F4	F8	1C	3B
64	66	E1	F6
F2	0D	4D	EC
DF	52	EB	79

Jika didalam bentuk ASCII maka didapat ciperteks : à d ò ß ø f R á M Ë; Ö Ì Y

Untuk mengubah kembali ciperteks menjadi plainteks maka dilakukan proses dekirpsi dengan menggunakan transformasi invers semua tranformasi dasar yang digunakan pada algoritma enkripsi AES. Setiap transformasi dasar AES memiliki transformasi invers yaitu L: *insubbytes, insvshiftrows,* dan *invmixcolumns.*

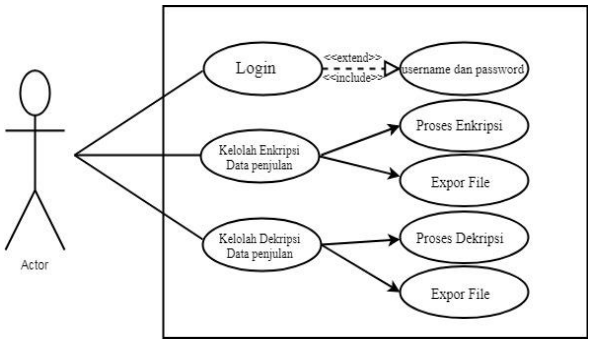
4. PEMODELANDAN PERANCANGAN SISTEM

4.1 Pemodelan Sistem

Pemodelan sistem merupakan gambaran sebuah perancangan dari sistem yang akan dibangun. Adapun diagram yang digunakan adalah pemodelan sistem dari UML (*Unified Modeling Language*), *Use Case diagram, Activity Diagram* dan *Class Diagram.*

4.1.1 *Use case diagram*

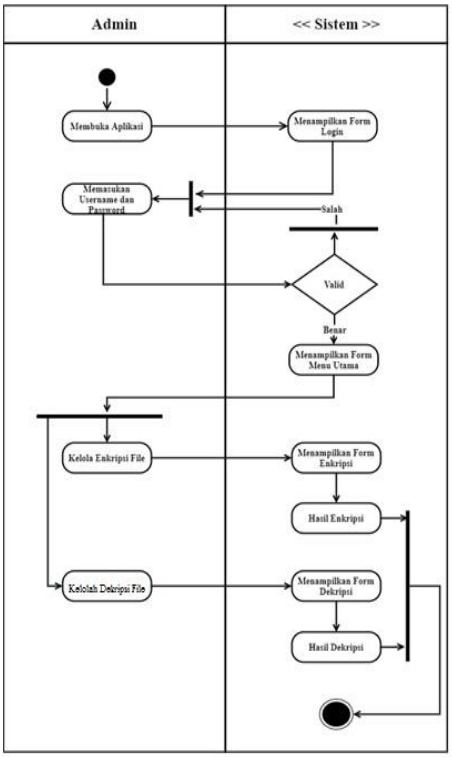
Berikut adalah gambar *Use case diagram* dari perancangan aplikasi Kriptografo AES untuk Mengenkripsi dan Mendekripsi data penjualan yaitu sebagai berikut:



Gambar 4.1 *Use Case Diagram Enkripsi* dan Dekripsi

4.1.2 *Activity diagram*

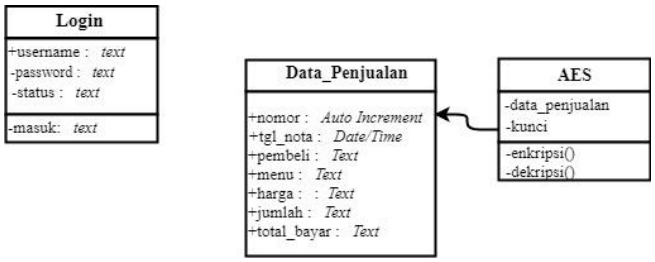
Activity Diagram digunakan untuk menggambarkan aliran aktivitas yang dilakukan sistem dan yang terjadi pada *use case* tertentu di dalam *use case diagram*. Dalam hal ini, yang akan dideskripsikan melalui *activity diagram*



Gambar 4.2 *Activity Diagram* Sistem

4.1.3 *Class Diagram*

Class Diagram biasa digunakan untuk menggambarkan struktur statis *class* di dalam sistem. *Class* merepresentasikan sesuatu yang ditangani sistem. Berikut adalah gambar *class diagram* yang digunakan di dalam sistem.



Gambar 4.3*Class Diagram* Sistem

5. PENGUJIAN DAN IMPLEMENTASI

5.1 Pengujian

Dalam implementasi dan pengujian didalam sistem pakar ini membutuhkan 2 buah perangkat yaitu, perangkat lunak dan perangkat keras.

Perangkat keras yang dibutuhkan dalam penelitian ini adalah sebagai berikut :

1. Komputer PC dengan *processor* mulai dari intel i3
2. RAM 2 GB
3. Mouse
4. Hardisk Minimal 320 Gb
5. Monitor
6. Keynoard

Perangkat lunak yang dibutuhkan dalam penelitian ini adalah sebagai berikut :

1. Sistem Operasi *Windows*7.
2. *Microsoft Visual Basic 2010, Microsoft Acces 2008, Crystal Report 8.5, Draw* io.

5.2 Implementasi Sistem

Hasil tampilan antar muka adalah tahapan dimana sistem atau aplikasi siap untuk dioperasikan pada keadaan yang sebenarnya sesuai dari hasil analisis dan perancangan yang dilakukan, sehingga akan diketahui apakah sistem atau aplikasi yang dirancang benar-benar dapat menghasilkan tujuan yang dicapai.

1. Halaman Menu Utama

Menu utama adalah tampilan awal ketika *user* memasuki sistem. Halaman ini berisi tampilan *Login.*

Gambar 5.1 Halaman *Login*

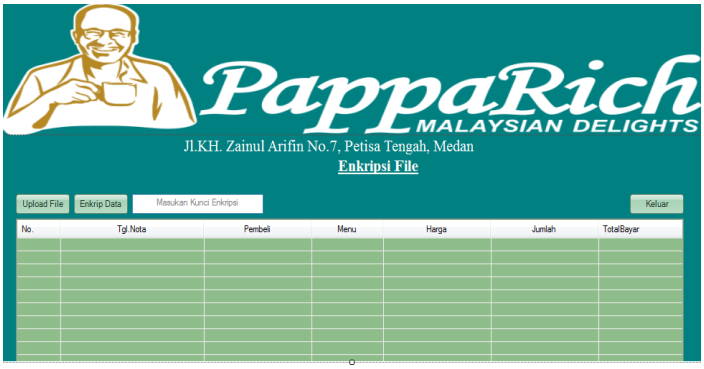
2. Halaman Menu Utama

Pada halaman utama ada beberapa f ungsional yang terdapat pada menu yaitu : *Button* Enkripsi File, *Button* Enkripsi File, *Button* Dekripsi File, *Button* Keluar.

Gambar 5.2 Halaman Menu Utama

3. Halaman Enkripsi File

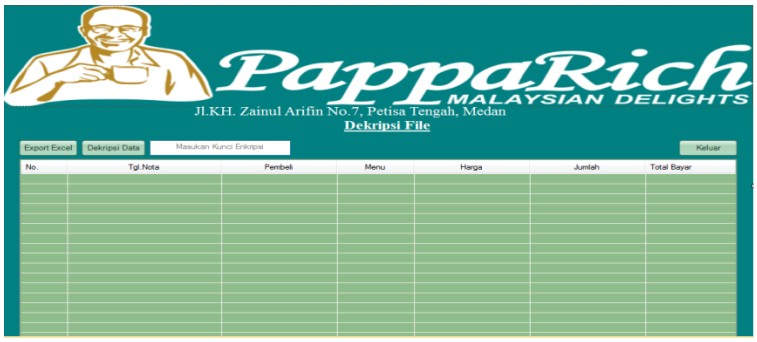
Halaman ini berfungsi untuk melakukan inpor data penjualan dan melakukan enkripsi data serta menyimpan kedalam *database* guna menjaga kerahasiaan data,



Gambar 5.3 Halaman Enkripsi file

4. Halaman Dekripsi File

Halaman ini berfungsi untuk melakukan dekripsi atau mengembalikan data yang sudah di emkripsi sebelumnya dan tersimpan di *database.*



Gambar 5.4 Halaman Dekripsi file

5.3 kelebihan dan kekurangan sistem

Adapun kelebihan dari sistem ini adalah sebagai berikut :

1. Sistem dapat melakukan keamanan data dengan waktu yang relatif efisien dan kemana data cukup baik untuk keamanannya.
2. Sistem dapat memberikan kemanan dan menjaga kerahasiaan data penjualanan untuk menghindari kecurangan yang terjadi.
3. Sistem sangat mudah digunakan.

Adapun kelemahan sistem ini adalah sebagai berikut :

1. Sistem belum memiliki form perubahan dan penambahan user pengguna.
2. Sistem yang digunakan hanya dapat menampung uploud data file excel.

6. Saran

Adapun saran dari penelitian ini yaitu:

Untuk meningkatkan kemampuan dan fungsi dari program ini ada beberapa saran yang dapat diberikan untuk pengembangan yang bisa dilakukan yaitu :

1. Program yang dibuat ini masih dapat dikembangkan lebih lanjut supaya menjadi sistem yang lebih lengkap berdasarkan dengan kepentingan yang lebih luas.
2. Agar kedepannya dapat mengembangkan sistem dengan bahasa pemograman *web* atau *mobile*
3. Agar kedepannya dapat melakukan proses tidak hanya bebrbentuk file excel saja.

UCAPAN TERIMA KASIH

Pada Kesempatan ini ucapan terimah kasih yang sedalam-dalamnya dan setinggi-tingginya kepada kedua orang tua saya, bapak Suriono dan ibu Siti Aminah yang telah memberi bantuan dan bimbingan baik berupa materi, motivasi, dan saran-saran yang tak terhingga.

Ucapan terima kasih yang sebesar-besarnya juga di berikan kepada yang terhormat:

1. Bapak Dr.Rudi Gunawan, S.E., M.Si.,selaku Ketua STMIK Triguna Dharma Medan.
2. Bapak Mukhlis Ramadhan, SE., M.Kom., selaku Wakil Ketua I (WAKA I) Bidang Akademik STMIK Triguna Dharma Medan.
3. Bapak Puji Sari Ramadhan,S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi STMIK Triguna Dharma Medan.
4. Bapak Nurcahyo Budi Nugroho., S.Kom., M.Kom., selakuDosen Pembimbing I yang telah meluangkan waktu, dan memberikan arahan dan saran untuk membimbing dalam menyelesaikanSkripsi ini.
5. Bapak Rico Imanta Ginting., S.Kom., M.Kom.,selakuDosen Pembimbing II yang telah meluangkan waktu, dan memberikan arahan dan saran untuk membimbing dalam penulisan Skripsi ini.
6. Bapak/Ibu Dosen dan seluruh Staf STMIK Triguna Dharma Medan yang telah memberikan ilmunya selama di perkuliahan.
7. Kepada Bapak Diki Zurlkarnaen yang membantu kelancaran riset pada PT. PappaRich Medan

REFERENSI

[1] mas'ud waqiah Nurul, "済無No Title No Title," *Persepsi Masy. Terhadap Perawatan Ortod. Yang Dilakukan Oleh Pihak Non Prof.*, vol. 53, no. 9, pp. 1689–1699, 2013.

[2] Y. Yanti, "Teknik Pengamanan File Dokumen Berbasis Text Menggunakan Metode Advanced Encryption Standard (AES)," *Semin. Nas. II USM 2017 Eksplor. Kekayaan Marit. Aceh di Era Glob. dalam Mewujudkan Indones. sebagai Poros Marit. Dunia*, vol. 1, pp. 87–90, 2017.

[3] A. L. Belakang, "No Title," pp. 1–5.

[4] A. H. Kridalaksana, E. Arriyanti, and W. Widodo, "Aplikasi Pengaman Sms Dengan Metode Kriptografi Advanced Encryption Standard (Aes) 128 Berbasis Android," *Sebatik*, vol. 10, no. 1, pp. 8–14, 2018, doi: 10.46984/sebatik.v10i1.59.

[5] S. Setti, I. Gunawan, B. E. Damanik, S. Sumarno, and I. O. Kirana, "Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 182, 2020, doi: 10.30865/jurikom.v7i1.1960

BIOGRAFI PENULIS

	**Nama : Dian Pratomo** **Nirm : 2017020833** **Program Studi : Sistem Informasi** **Tempat/Tgl. Lahir : Balimbinggan, 14 Juli 1998** **Agama : Islam** **Jenis Kelamin : Laki-laki** **No/Hp : 083107336115** **Email : ddsdianpratomo1407@Gmail.Com** **Deskripsi : Mahasiswa Stambuk 2017. Saat Ini Sedang Menempuh Pendidikan Strata-1 (S1) Di STMIK Triguna Dharma.**
	**Nama : Nurcahyo Budi Nugroho, S.Kom, M.Kom.** **Nidn : 0130038201** **Agama : Islam** **Jenis Kelamin : Laki-Laki** **No/Hp : 085831511117** **Email : nurcahyobn@Gmail.Com** **Bidang Keilmuwan : Keamanan Komputer**
	**Nama : Rico Imanta Ginting, S.Kom, M.Kom.** **Nidn : 0102029002** **Agama : Islam** **Jenis Kelamin : Laki-Laki** **No/Hp : 085277915778** **Email : icoversi90@gmail.com** **Bidang Keilmuwan : Kecerdasan Buatan**