APLIKASI KRIPTOGRAFI DATABASE DENGAN METODE AES128 DAN VIGENERE CIPHER PADA PT. SATRINDO MITRA UTAMA

Aji Putra Pratama[1)], **Sri Mulyati**[2)]
[1]Program studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : jibonslop@gmail.com [1)], sri.mulyati@budiluhur.ac.id [2)]

Abstrak

PT. SATRINDO MITRA UTAMA Jakarta merupakan suatu perusahan yang bergerak di bidang distributor traktor pertanian danpertanian. IT yang memiliki database yang berisi data Barang, data customer dan data transaksi. Hal yang terjadi pada PT.satrindo mitra utama adalah data yang tersimpan di database masih sama dengan data yang user input ssehingga itu bisa menyebabkan terjadi percurian data pada PT. satrindo mitra utama sehingga memerlukan teknik pengamanan di dalama database. Teknik pengamanan ini mengimplementasikan kriptografi. Kriptografi yang digunakan pada penelitian ini yaitu AES128 DAN VIGENERE CIPHER. Pada jurnal ini penulis berusaha membuat suatu aplikasi pengamanan database dengan menggunakan metode algoritma kriptografi AES128 DAN VIGENERE CIPHER. Aplikasi pengamanan database yang berbasis desktop menggunakan bahasa pemrograman Java. Dengan adanya aplikasi ini, penulis berharap agar pengguna dapat menyimpan data yang bersifat secara rahasia ke dalam database tanpa perlu takut ada orang lain bisa dapat membaca isi dari data tersebut.oleh karena itu di butuhkan apli kasi yang dapat memuddahkan penguna menggunakanya.dan maka dari itu di buatnya aplikasi ini dengan menggunakan metode AES 128 dan Vigenere cipher

Kata kunci: Algoritma AES128, VIGENERE CIPHER, Kriptografi, *Database*

1. PENDAHULUAN

Seiring dengan perkembangannya teknologi dan komunikasi tersebut, Salah satu dampak perkembangan negatif dalam perkembangan teknologi adalah pencurian data, yang merupakan salah satu masalah yang paling ditakuti oleh jaringan komunikasi dan informasi. Dengan adanya pencurian data maka aspek keamanan dalam pertukaran informasi serta penyimpanan data di anggap penting.

PT. SATRINDO MITRA UTAMA Jakarta merupakan salah satu perusahan swasta yang memiliki data-data yang sangat penting yang disimpan dalam suatu *database*. oleh karena itu PT. SATRINDO MITRA UTAMA Jakarta membutuhkan sebuah aplikasi pengamanan untuk membantu mengamankan data-data penting agar tidak diketahui oleh orang lain dan disalah gunakan oleh orang yang tidak bertanggung jawab.

Dengan demikian maka dibutuhkan suatu sistem pengamanan yang memiliki tingkat kemanan yang cukup tinggi untuk menjamin kerahasian data atau informasi penting tersebut agar tidak dicuri atau dimanipulasi. Dengan cara menjaga kerahasiaan data penting tersebut dan menyembunyikannya. Kriptografi adalah salah satu metode yang digunakan dalam penelitian ini untuk merahasiakan data penting tersebut.

Pada penelitian ini algoritma yang di pakai yaitu algoritma AES 128 dan *Vigenere Cipher*. Dengan menggunakan kedua metode ini diharapkan memiiki tingkat keamanan yang sangat cukup tinggi semoga dapat menjaga keamanan atau kerahasiaan data pada *database* supaya tidak mudah dicuri atau di ambil oleh pihak yang tidak bersangkut pautan pada perusahan tersebut..

Dengan melihat latar belakang diatas maka dapat diambil dengan beberapa pokok permasalahan yang dimiliki oleh PT. SATRINDO MITRA UTAMA Jakarta. bagaimana membuat sebuah pengamanan untuk data dalam *database* yang besifat rahasia agar tidak diketahui oleh orang yang tidak bertanggung jawab. Dibuatnya pengamanan pada *database* agar informasi didalamnya tidak semua orang dapat mengetahuinya. Pengamanan tersebut dibutuhkan karena informasi tersebut berisikan data penting PT. SATRINDO MITRA UTAMA Jakarta.

2. METODE PENELITIAN

2.1. Algoritma *Vigenere Cipher*

Pada vigenere cipher, kunci yang digunakan berupa karakter yang dimasukan oleh pengguna. Karakter yang digunakan pada vigenere cipher disini yaitu a, b, c, ..., z, A, B, C, ..., Z, 0, 1, 2, 3, ..., 9, dan karakter simbol lainnya seperti pada Tabel 1 tersebut. Proses enkripsi dimulai dengan menyesuaikan setiap huruf dengan angka 0 sampai 92. Dan hasil enkripsi didapatkan dari menambahkan nilai pesan dengan kunci. Hasil akan dikurangi 93 apabila nilai hasil lebih dari 92. Model matematis algoritma enkripsi vigenere cipher dapat dihitung dengan menggunakan persamaan : [1]

2.2. Algoritma AES

Dalam proses enkripsi input, diperlukanlah empat macam operasi yang dilakukan berulang-ulang dalam beberapa putaran dan menggunakan kunci *cipher*. Jumlah putaran yang digunakan algoritma ini ada tiga macam seperti pada tabel di bawah ini. [3]

Tabel 2. Perbandingan Panjang Kunci AES

Tipe	Jumlah key (Nk)	Besar Blok (Nb)	Jumlah Round (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Setiap tipe menggunakan kunci yang berbeda yaitu *round key* untuk setiap proses perhitungan putaran. Setiap putaran enkripsi AES-128 bit dikerjakan dalam 10 kali) a=10), yaitu sebagai berikut.

a. Addroundkey.
b. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap proses putaran adalah: *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*.
c. *Final round*, adalah proses untuk putaran terakhir yang meliputi *SubBytes*, *ShiftRows*, dan *AddRoundKey [2]*

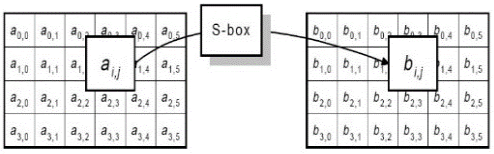
2.3. Proses Enkripsi AES 128

Proses enkripsi pada algoritma *Advanced Encryption Standard* (AES) terdiri dari empat operasi yaitu *Add Round Key, Sub Bytes, Shift Rows*, dan *Mix Columns*. Operasioperasi ini diulang terus-menerus hingga menghasilkan *ciphertext*. Jumlah perulangan yang dilakukan tergantung pada ukuran blok dan kunci yang digunakan, dalam hal ini ukuran blok dan kunci yang digunakan yaitu 128 bit, sehingga berdasarkan pada teori, maka perulangan/ronde yang dilakukan sebanyak 10 kali.

Contoh analisis enkripsi pada algoritma AES (*Advanced Encryption Standard) 128 bit*, jika diketahui kunci dan plaintext yang akan digunakan untuk enkripsi dengan panjang 16 byte, sebagai berikut : [2]

1) SubByte

Proses mensubstitusi *plaintext* yang telah diekspansi ke dalam S-Box.



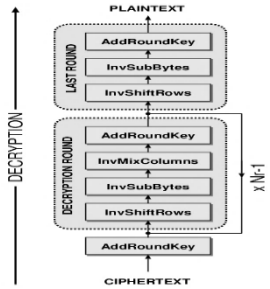
Gambar 1. Ilustrasi transformasi SubByte

Tabel 3. S-Box Algoritma AES

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

2.4. Proses dekripsi AES

Perubahan *byte* yang digunakan pada *invers cipher* adalah *InvMixColumns*, *AddRoundKey*,, *InvShiftRows* , dan *InvSubBytes*. Algoritma dekripsi tersebut dapat dilihat pada skema seperti berikut ini :



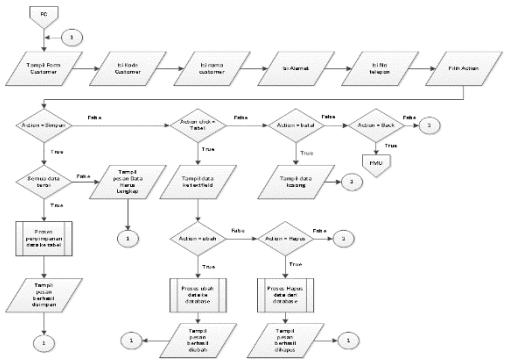
Gambar 2. Alur proses dekripsi algoritma

3. HASIL DAN PEMBAHASAN

3.1. Analisa Masalah

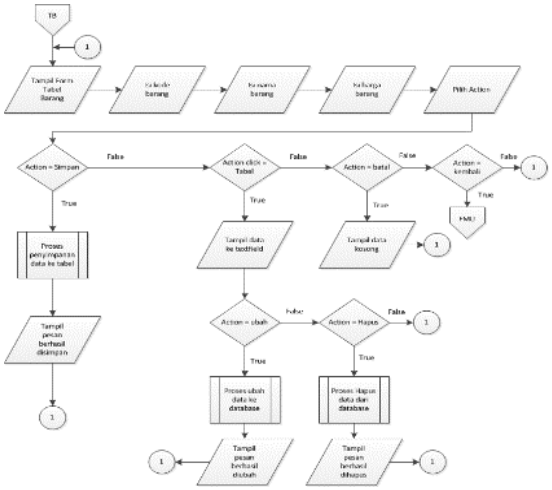
Pada PT. Satrindo Mitra Utama memiliki informasi yang tidak boleh diketahui oleh orang lain. Kerahasiaan suatu informasi tersebut, selalu menjadi masalah tersendiri bagi PT. Satrindo Mitra Utama. Dimana data Custemer,Barang dan Transaksi yang dihasilkan PT. Satrindo Mitra Utama, harus bisa diamankan. Tanpa pengamanan yang maksimal, maka kerugian akan dialami PT. Satrindo Mitra Utama tersebut manakala informasi yang sangat penting dan rahasia tersebut hilang atau dicuri oleh orang yang tidak bertanggung jawab.

3.2 Flowchart



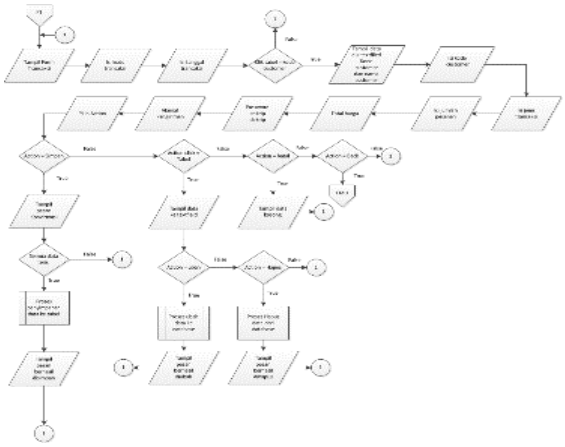
Gambar 3. *Flowchart* Halaman Menu Customer

Flowchart ini menjelaskan alur proses dari halaman menu customer.menu customer merupakan menu yang berfungsi untuk menginput, mengubah ataupun menghapus data customer.



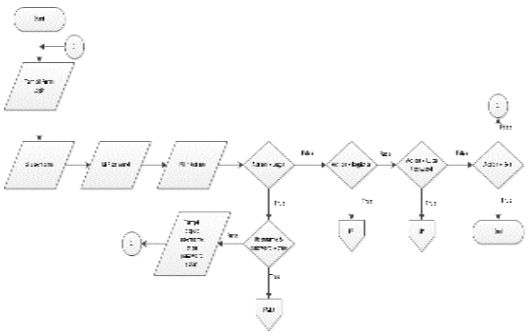
Gambar 4. *Flowchart* Halaman Menu Barang

Flowchart ini menjelaskan alur proses dari halaman menu barang. Menu barang merupakan menu yang berfungsi untuk menginput, mengubah ataupun menghapus data barang



Gambar 5. *Flowchart* Halaman Menu Transaksi

Flowchart ini menjelaskan proses tampilan halaman menu Transaksi dari aplikasi kriptografi

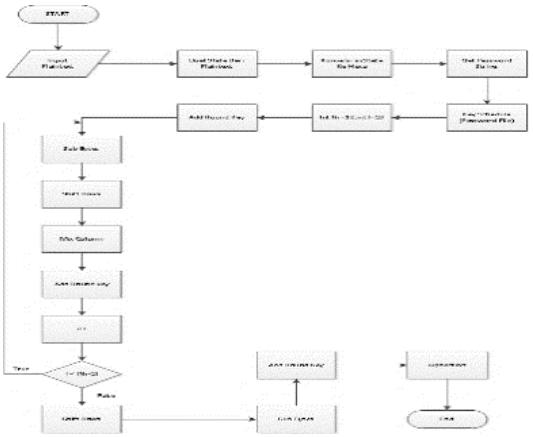


Gambar 3.17: *Flowchart* Halaman Menu *Login*

Halaman ini terdapat menu *login* untuk *user* apabila ingin masuk kedalam menu utama. *Flowchart* halaman menu *login* seperti gambar 3.17 berikut:

3.3 *Flowchart* Enkripsi Aes 128

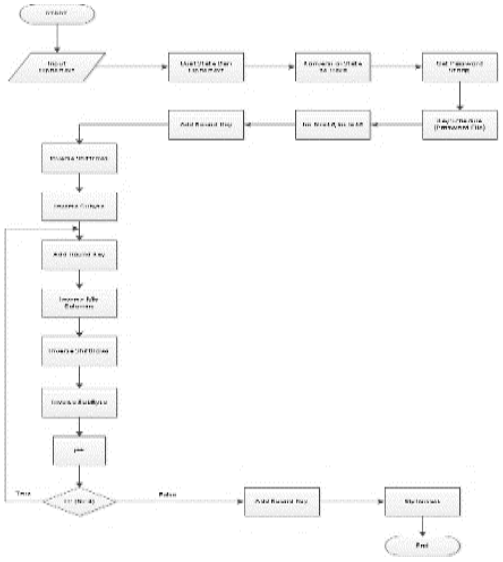
Flowchart proses enkripsi AES 128 merupakan gambaran alur sebuah *database* yang akan mengalami proses.



Gambar 6. *Flowchart* Proses Enkripsi AES 128

3.4. *Flowchart* Deskripsi AES 128

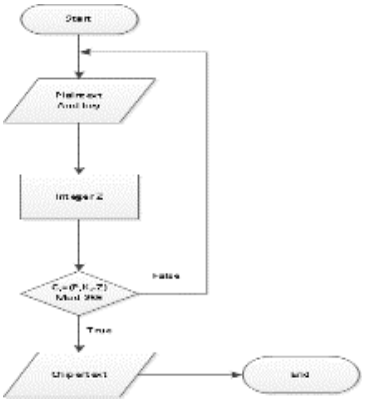
Flowchart proses dekripsi Aes 128l merupakan gambaran alur sebuah *database* yang akan mengalami proses dekripsi (pengembalian isi *database*)



Gambar 7. *Flowchart* Proses Dekripsi AES 128

3.5. *Flowchart* Enkripsi Vigenere chipper

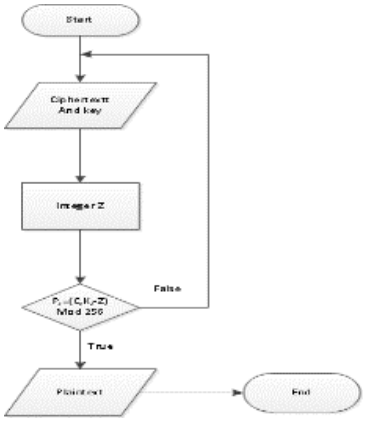
Flowchart proses enkripsi vigenere chipper merupakan gambaran alur sebuah *database* yang akan mengalami proses



Gambar 8. *Flowchart* Proses Enkripsi Vigenere chipper

3.6 Flowchart Deskripsi Vigenere chipper

Flowchart proses enkripsi vigenere chipper merupakan gambaran alur sebuah *database* yang akan mengalami proses.

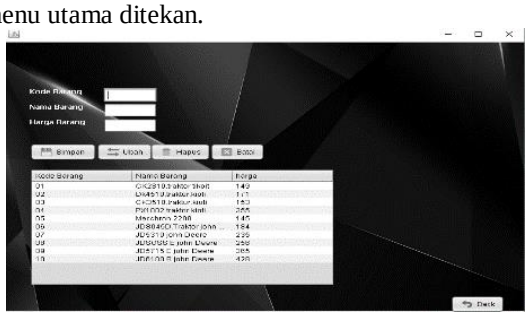


Gambar 9. *Flowchart* Proses Dekripsi Vigenere Chipper

4. IMPLEMENTASI DAN UJI COBA PEROGRAM

4.1. Tampilan Layar Form Barang

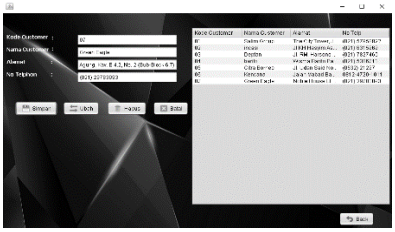
Tampilan layar *form* Barang pada gambar 10 ini muncul pada saat *button* Barang yang berada di menu utama ditekan.



Gambar 10 : Tampilan Layar *Form* Barang

4.2. Tampilan Layar Form Customer

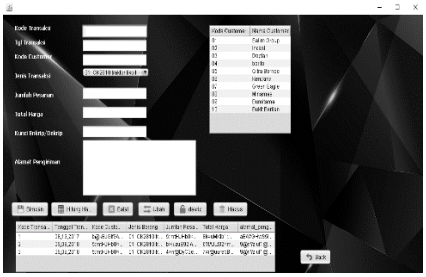
Tampilan layar *form* Customer pada gambar 11 ini muncul pada saat *button* Customer yang berada di menu utama ditekan.



Gambar 11 : Tampilan Layar *Form* Customer

4.3. Tampilan Layar Form Transaksi

Tampilan *form Transaksi* ini akan tampil pada saat *button Transaksi* yang berada di menu utama ditekan.



Gambar 12 : Tampilan Layar *Form Transaksi*

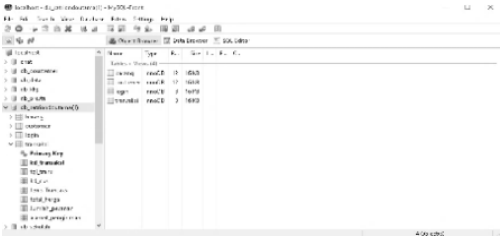
4.4. Tampilan layar Gagal Di Dekrip

Tampilan layar *From* menu transaksi pada saat data Transaksi gagal di dekrip 13. pengguna tidak memasukan password yang sama pada saat mengenkripsi sebelumnya.

Gambar 13 : Tampilan From Transaksi gagal di Dekrip

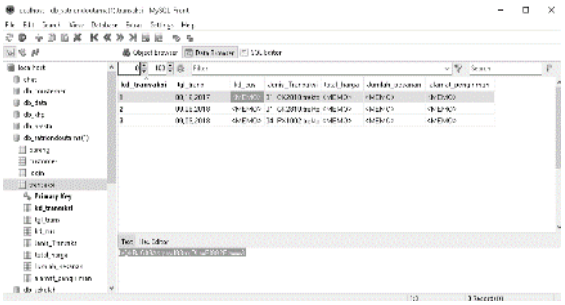
4.5. Enkripsi dan Dekripsi Database

Untuk melakukan proses enkripsi *database* pengguna dapat memilih tombol enkripsi pada masing-masing *form* yang telah disediakan tombol enkripsi. Pada gambar 11 memperlihatkan tampilan awal isi dari database db_satriondoutama(1) yang akan dienkripsi.



Gambar 14. Tampilan Isi dari *Database* db_satriondoutama(1)

Pada gambar 11 memperlihatkan isi *table* Transaksi dari *database* db_satriondoutama(1) yang telah terenkripsi.



Gambar 15. Tampilan Isi dari *Table* Transaksi

4.6. Evaluasi Program

Setelah melakukan analisa tersebut dari hasil aplikasi pengujian maka dapat ditemukan beberapa kelebihan dan kekurangannya dari aplikasi ini, yaitu sebagai berikut:

Kelebihan Program

1) Program aplikasi ini mudah dikelola dan digunakan.
2) Dapat digunakan oleh siapapun untuk mengamankan isi *database.*
3) Database yang sudah terenkripsi tidak dapat dibaca lagi.
4) Isi database tidak mengalami perubahan setelah didekripsi kembali.

Kekurangan Program

1) Semakin besar suatu ukuran *database tersebut* yang ingin dienkripsi maka waktu yang dibutuhkan semakin lama.
2) *User* yang menggunakan aplikasi ini harus mengerti *database.*

Jika ingin mendekripsi, harus hafal kunci yang dimasukan pada enkripsi *database* sebelumnya.

4.7. Tabel Pengujian

Tabel 4. Hasil Pengujian Tabel *Transaksi*

Nama Data	Karakter Asli	jumlah	Karakter Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi
Kd_transaksi	1	1	-	-
Tgl_trans	08,19,20	10	-	-
	17			
Kd_cus	01	2	b@kBJGIf9A<qwyJ83m;DLwBf99?Eww3	32
Jenis_transaksi	01 CK2810.traktor tikoit	2	-	-
Total_harga	1490		8k=uMKIb1:@HDxHf6=nAxvH27k?uvwA9	32
Jumblah_pesanan	10		5:mtHJHb0<8DHuu0bn<BMKA70k>GKKta	32
alamat_pengirim	The City Tower, Jl. M.H. Thamrin No.81	8	aBA?GHw95l?FGGr6d;>Awwt81?iHyKu4bk8AFCs88Aj?xyr3c;@FuvEffl?AyKv8c@??Exv02n@ryKC05omFEFw649m?wtJ9	94

4.8. Evaluasi Perogram

Setelah dilakukan Analisa dari hasil pengujian aplikasi ini terdapat beberapa kelebihan dan kekurangannya dari aplikasi ini, yaitu sebagai berikut:

a. Kelebihan Perogram
   1) Aplikasi mudah dikelola dan digunakan.
   2) Dapat digunakan oleh siapapun untuk mengamankan isi *database.*
   3) Database yang sudah terenkripsi tidak dapat dibaca lagi.
   4) Isi database tidak mengalami perubahan setelah didekripsi kembali.

b. Kekurangan Perogram
   1) Semakin besar ukuran *database* yang ingin dienkripsi maka waktu yang dibutuhkan semakin lama.
   2) *User* yang menggunakan aplikasi ini harus mengerti *database.*

3) Jika ingin mendekripsi, harus hafal kunci yang dimasukan pada enkripsi *database* sebelumnya.

5. KESIMPULAN

Berdasarkan analisa yang telah saya lakukan kepada permasalahan dan aplikasi yang sedang dikembangkan, dapat ditapsirkan kesimpulan, sebagai berikut:

a. Enkripsi AES 128 dan Vigenere cipher ini dapat mengimplementasikan pada aplikasi pengamanan database dengan menggunakan pemograman java dan database MySQL

b. Aplikasi ini dapat dijalankan sesuai dengan spesifikasi teknis yang sudah dirancang.dengan sedemikian rupa

c. Aplikasi ini dapan mengamankan data yang masuk kedalam sebuah database dengan menggunakan teknik kriptografi menggunakan metode AES 128 dan Vigenere cipher sehingga sebuah data yang tersimpan ke dalam database akan sulit di baca

DAFTAR PUSTAKA

[1] (Ariska et al., 2018)Ariska, B., Endri, J., Studi, P., Telekomunikasi, T., Teknik, J., Negeri, P., & Palembang, S. (2018). Rancangan Kriptografi Hybrid Kombinasi Metode Vigenere Cipher Dan Elgamal Pada Pengamanan Pesan, 328–336.

[2] Herwanto, P., & Tris. (2016). Jurnal Informasi Volume VIII No.1 / Februari / 2016. *Jurnal Informasi*, *VIII*(1), 1–22.

[3] Madaharsa, B., & Adiwidya, D. (n.d.). Algoritma AES (Advanced Encryption Standard) dan Penggunaannya dalam Penyandian Pengompresian Data.

[4] (Herwanto & Tris, 2016)(Madaharsa & Adiwidya, n.d.)