IMPLEMENTASI ALGORITMA KRIPTOGRAFI *TRIANGLE CHAIN CIPHER (TCC)* UNTUK PENGAMANAN *DATABASE* BERBASIS *DESKTOP* PADA CV. USAHA TANI

Sani Akazar Pebresega[1)], Dewi Kusumaningsih[2)]
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : [1)]saniakazar1@gmail.com, [2)]dewi.kusumaningsih@budiluhur.ac.id

ABSTRAK

CV.Usaha Tani adalah sebuah lembaga yang bekerja pada bidang pertanian. Banyak database yang bersifat rahasia dan tidak boleh di ketahui oleh pihak yang tidak berhak untuk melihatnya. Oleh karena itu, untuk mengamankan tabel database kita dapat menggunakan kriptografi, pengguna tabel database membutuhkan bantuan keamanan akan tabel database yang akan disimpannya. Penerapan kriptografi pada CV.Usaha Tani akan di fokuskan bagaimana sampai dengan database dibuka oleh pihak yang berhak untuk melihatnya. Algoritma yang digunakan oleh penulis adalah Triangle Chain. Oleh karena itu dibutuhkan aplikasi yang dapat memudahkan pengguna untuk menginput dan menyimpan data-data tersebut dengan aman dan terjaga kerahasiaannya. Pada penelitian ini penulis mengimplementasikan keamanan data pada database. Teknik pengamanan data ini dilakukan dengan menggunakan teknik kriptografi TCC (Triangle Chain Cipher). Algoritma kriptografi TCC (Triangle Chain Cipher) dapat dimanfaatkan untuk mengamankan data serta memberikan kemudahan kepada user untuk mengamankan datanya supaya isi dari data tersebut tidak diketahui oleh pihak yang tidak memiliki kepentingan terhadap data tersebut. Pada tugas akhir ini penulis berusaha untuk membuat suatu aplikasi pengamanan database dengan menggunakan algoritma kriptografi TCC (Triangle Chain Cipher). Aplikasi pengamanan database ini berbasis desktop menggunakan bahasa pemrograman VB.net. Dengan adanya aplikasi ini, penulis berharap agar pengguna dapat menyimpan data yang bersifat rahasia ke dalam database tanpa takut ada orang lain yang dapat membaca isi dari data tersebut.

Kata kunci : Algoritma TCC (*Triangle Chain Cipher*), Kriptografi, *Database*.

1. PENDAHULUAN

Salah satu dampak perkembangan negatif dalam perkembangan teknologi adalah ada pencurian data, yang merupakan salah satu masalah yang paling di takuti oleh Jaringan komuikasi. Dengan adanya pencurian data maka aspek keamanan dalam pertukaan informasi serta penyimpanan data di anggap penting. CV.Usaha Tani adalah sebuah lembaga yang bekerja pada bidang pertanian. Banyak *database* yang bersifat rahasia dan tidak boleh di ketahui oleh pihak yang tidak berhak untuk melihatnya. Oleh karena itu, untuk mengamankan tabel *database* kita dapat menggunakan kriptografi. Pengguna tabel *database* membutuhkan bantuan keamanan akan tabel *database* yang akan disimpannya. Penerapan kriptografi pada CV.Usaha Tani akan di fokuskan bagaimana cara mengamankan *database* dengan ilmu kriptografi ini sehingga *database* tidak bisa dibaca, kemudian bisa dibaca kembali oleh pihak yang berhak untuk melihatnya.

2. LANDASAN TEORI

2.1 Kriptografi

Kiptografi sebuah teori keamanan untuk menjaga kerahasiaan pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti orang lain, selain pemilik data tersebut (Jumrin, 2016) [1].

Kriptografi pengetahuan yang berguna untuk mengacak data semedikian rupa sehingga tidak bisa dibaca oleh pihak ketiga (Kromodimoeljo,2009) [2].

Seiring perkembangan kriptogarfi digunakan untuk keamanan komunikasi penting seperti komunikasi dikalangan masyarakat umum untuk melindungi data yang bersifat pribadi (Basri, 2016) [3].

(Hasrul, 2016([4]. Aspek-aspek keamanan di dalam kriptografi meliputi :

1) *Confidentiality* (Kerahasiaan)
2) Data *Integrity* (Integritas)
3) *Authentication* (Otentikasi)
4) Non-*repudiation* (Penyangkalan)

2.2 Algoritma triangle chain (TCC)

Pengolahan kode rahasia yang diproses algoritma TCC berupa *cipher* segitiga dua kali lipat serta melakukan enkripsi ganda, dengan cara membuat pola enkripsi pertama ke arah kanan dan enkripsi kedua ke arah kiri.

Tabel 1 : Tabel Kode ASCII 0~127

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	NUL	31	1F	US	61	3D	=	91	5B	[	121	79	y	151	97	–	181	B5	µ	211	D3	Ó	241	F1	ñ
1	01	SOH	32	20	SP	62	3E	>	92	5C	\	122	7A	z	152	98	˜	182	B6	¶	212	D4	Ô	242	F2	ò
2	02	STX	33	21	!	63	3F	?	93	5D	]	123	7B	{	153	99	™	183	B7	·	213	D5	Õ	243	F3	ó
3	03	ETX	34	22	"	64	40	@	94	5E	^	124	7C	|	154	9A	š	184	B8	¸	214	D6	Ö	244	F4	ô
4	04	EOT	35	23	#	65	41	A	95	5F	_	125	7D	}	155	9B	›	185	B9	¹	215	D7	×	245	F5	õ
5	05	ENQ	36	24	$	66	42	B	96	60	`	126	7E	~	156	9C	œ	186	BA	º	216	D8	Ø	246	F6	ö
6	06	ACK	37	25	%	67	43	C	97	61	a	127	7F	[]	157	9D		187	BB	»	217	D9	Ù	247	F7	÷
7	07	BEL	38	26	&	68	44	D	98	62	b	128	80	€	158	9E	ž	188	BC	¼	218	DA	Ú	248	F8	ø
8	08	BS	39	27	'	69	45	E	99	63	c	129	81		159	9F	Ÿ	189	BD	½	219	DB	Û	249	F9	ù
9	09	HT	40	28	(	70	46	F	100	64	d	130	82	‚	160	A0		190	BE	¾	220	DC	Ü	250	FA	ú
10	0A	LF	41	29	)	71	47	G	101	65	e	131	83	ƒ	161	A1	¡	191	BF	¿	221	DD	Ý	251	FB	û
11	0B	VT	42	2A	*	72	48	H	102	66	f	132	84	„	162	A2	¢	192	C0	À	222	DE	Þ	252	FC	ü
12	0C	FF	43	2B	+	73	49	I	103	67	g	133	85	…	163	A3	£	193	C1	Á	223	DF	ß	253	FD	ý
13	0D	CR	44	2C	,	74	4A	J	104	68	h	134	86	†	164	A4	¤	194	C2	Â	224	E0	à	254	FE	þ
14	0E	SO	45	2D	-	75	4B	K	105	69	i	135	87	‡	165	A5	¥	195	C3	Ã	225	E1	á	255	FF	ÿ
15	0F	SI	46	2E	.	76	4C	L	106	6A	j	136	88	ˆ	166	A6	¦	196	C4	Ä	226	E2	â			
16	10	DLE	47	2F	/	77	4D	M	107	6B	k	137	89	‰	167	A7	§	197	C5	Å	227	E3	ã			
17	11	DC1	48	30	0	78	4E	N	108	6C	l	138	8A	Š	168	A8	¨	198	C6	Æ	228	E4	ä			
18	12	DC2	49	31	1	79	4F	O	109	6D	m	139	8B	‹	169	A9	©	199	C7	Ç	229	E5	å			
19	13	DC3	50	32	2	80	50	P	110	6E	n	140	8C	Œ	170	AA	ª	200	C8	È	230	E6	æ			
20	14	DC4	51	33	3	81	51	Q	111	6F	o	141	8D		171	AB	«	201	C9	É	231	E7	ç			
21	15	NAK	52	34	4	82	52	R	112	70	p	142	8E	Ž	172	AC	¬	202	CA	Ê	232	E8	è			
22	16	SYN	53	35	5	83	53	S	113	71	q	143	8F		173	AD	-	203	CB	Ë	233	E9	é			
23	17	ETB	54	36	6	84	54	T	114	72	r	144	90		174	AE	®	204	CC	Ì	234	EA	ê			
24	18	CAN	55	37	7	85	55	U	115	73	s	145	91	'	175	AF	¯	205	CD	Í	235	EB	ë			
25	19	EM	56	38	8	86	56	V	116	74	t	146	92	'	176	B0	°	206	CE	Î	236	EC	ì			
26	1A	SUB	57	39	9	87	57	W	117	75	u	147	93	"	177	B1	±	207	CF	Ï	237	ED	í			
27	1B	ESC	58	3A	:	88	58	X	118	76	v	148	94	"	178	B2	²	208	D0	Ð	238	EE	î			
28	1C	FS	59	3B	;	89	59	Y	119	77	w	149	95	•	179	B3	³	209	D1	Ñ	239	EF	ï			
29	1D	GS	60	3C	<	90	5A	Z	120	78	x	150	96	–	180	B4	´	210	D2	Ò	240	F0	ð			
30	1E	RS																									
31	1F	US																									

2.2.1 Algortima Enkripsi TCC

Adapun algoritma enkripsi yang ada pada metode ini dengan menggunakan rumus sebagai berikut:

1. Matriks Enkripsi Segitiga Pertama
   Untuk baris ke-1 :
   M1j = P[j] + (K * R[1]) mod 255
   untuk baris ke-2 dan selanjutnya untuk nilai j ≥ i :
   Mij = M(i,j) + (K * R [i]) mod 255, sehingga nilai
   ciphertext yang diperoleh adalah :
   Mij = [j,(N+j)-n].
2. Matriks Enkripsi Segitiga Kedua
   Nilai P diperoleh dari nilai Mij pada i = j
   Untuk baris ke-1 :
   M1j = P[j] + (K*R[1])) mod 255
   untuk baris ke 2 dan selanjutnya untuk nilai j ≤
   (N+1) – i :
   Mij = M(i,j)+(K*R[i])) mod 255, sehingga nilai
   cipherteks yang diperoleh adalah :
   Mij = [(N-j)+1, j].

Keterangan :
P=Plainteks ; N=Jumlah Karakter Plainteks;
M=Matriks penampung hasil penyandian
K=Kunci; R= Row (baris perkalian faktor pengali dengan kunci); i= Index faktor pengali; j=Index karakter plaintext; Nilai R = M; J = R; i = R

2.2.2 Algoritma Dekripsi TCC

Sedangkan untuk algoritma dekripsi *Triangle Chain Cipher* merupakan kebalikan dari algoritma enkripsi, rumusnya sebagai berikut:

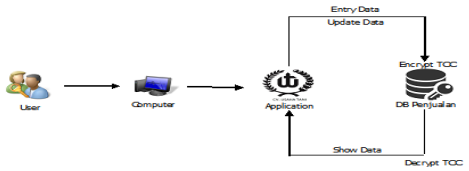
1. Matriks dekripsi segitiga pertama operasinya
   merupakan kebalikan dari matriks enskripsi, jadi
   operasi ini kebalikan operasi matriks enkripsi segitiga
   kedua. Nilai C merupakan tabel dari ciphertext dengan
   panjang N yaitu C[N].
   Mencari baris ke-1 :
   M1j = C[j] - (K * R[1]) mod 255
   untuk baris ke-2 dan selanjutnya untuk nilai j ≥ i :
   Mij = C(i,j) - (K * R [i]) mod 255
   Nilai ciphertext yang diperoleh adalah :
   Mij = [j,(N+j)-n].
2. Matriks dekripsi segitiga kedua
   Baris pertama berlaku formula, dengan nilai i = j
   Untuk baris ke-1 :
   M1j = C[j] - (K*R[1])) mod 255
   untuk baris ke 2 dan selanjutnya untuk nilai j ≤ (N+1) – i :
   Mij = M(i,j) - (K*R[i])) mod 255, sehingga nilai
   cipherteks yang diperoleh adalah :
   Mij = [(N-j)+1, j].

Keterangan : C=Ciphertext

3. ANALISA MASALAH DAN RANCANGAN APLIKASI

Tahapan-tahapan yang terjadi dalam proses sistem aplikasi ini dapat dijelaskan sebagai berikut. karena berfungsi sebagai gudang penyimpanan data yang akan diolah lebih mendalam karena dapat mengorganisasi data, menghidari duplikasi data, juga *update* yang rumit (Rahmad, 2014).

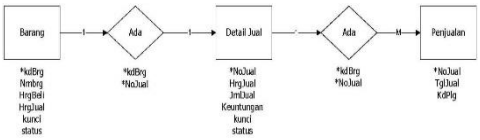
3.1 Arsitektur sistem



Gambar 1.Arsitektur Sistem

3.2 ERD (*Entity Relationship Diagram*)

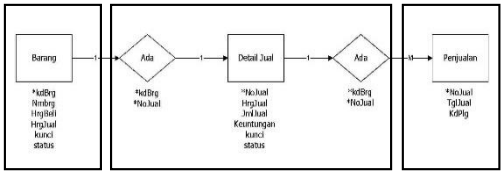
Kumpulan bagian dari keseluruhan suatu yang berwujud serta kumpulan penghubung antar pihak seluruh data yang ada. Seperti pada Gambar 3 adalah gambar rancangan ERD:



Gambar 2. ERD (*Entity Relationship Diagram*)

3.3 Transformasi *ERD* ke *Logical Record Structure* (LRS)

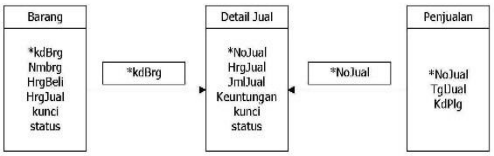
Berdasarkan ER-Diagram pada Gambar maka didapatkan
transformasi ER-Diagram ke *Logical Record Structure* sebagai berikut:



Gambar 3. Tansformasi ERD Ke LRS

3.4 *Logical Record Structure* (LRS)

Dari transFormasi ER-Diagram ke LRS yang dijabarkan pada gambar 3.3 maka dihasilkan bentuk *Logical Record Structure* (LRS) untuk aplikasi yang diusulkan sebagai berikut:



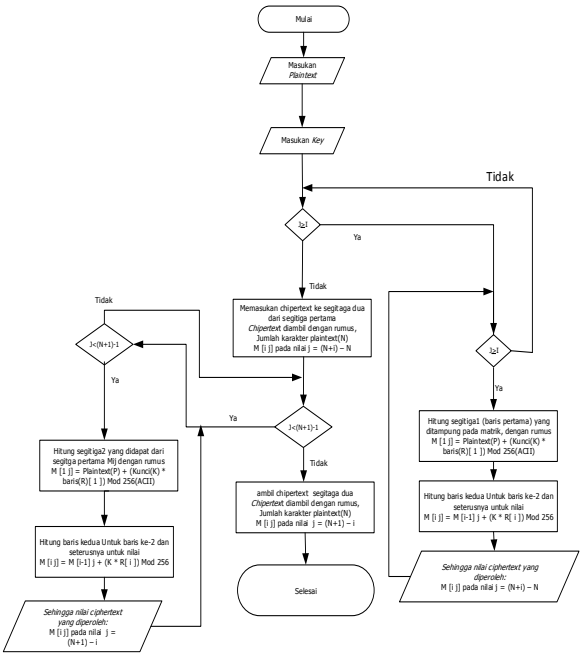
Gambar 4. *Logical Record Structure* (LRS)

3.5 Flowchart Aplikasi

Untuk memudahkan pemahaman proses, kerangka berfikir akan disajikan dalam bentuk *flowchart* sebagai berikut :

3.5.1 *Flowchart Enkripsi TCC (Triangle Chain Cipher)*

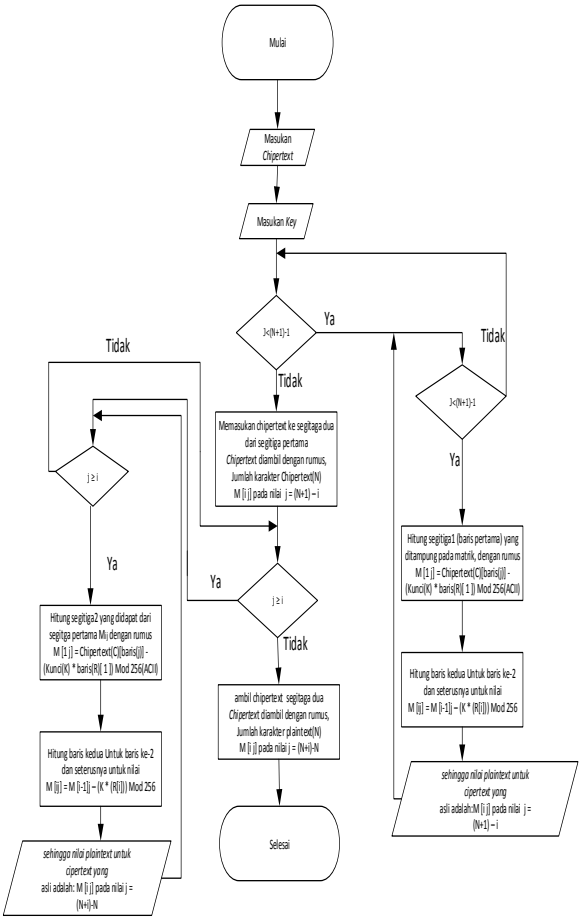
Flowachart proses Enkripsi TCC (*Triangle Chain Cipher*) menjelaskan alur proses atau cara kerja algoritma TCC (*Triangle Chain Cipher*) untuk menghasilkan *ciphertext.* Untuk lebih jelasnya berikut adalah proses dari *flowcahart* proses enkripsi TCC (*Triangle Chain Cipher*):



Gambar 5. Flowchart TCC Enkripsi

3.5.2 *Flowchart* Dekripsi TCC (*Triangle Chain Cipher*)

Flowachart proses Dekripsi TCC (*Triangle Chain Cipher*) menjelaskan alur proses atau cara kerja algoritma TCC (*Triangle Chain Cipher*) untuk menghasilkan *plaintext.* Untuk lebih jelasnya berikut adalah proses dari *flowcahart* proses enkripsi TCC (*Triangle Chain Cipher*):

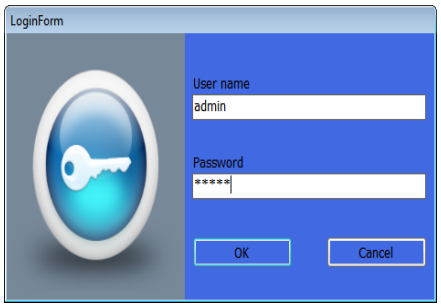


Gambar 6. Flowchart TCC Dekripsi

4. HASIL DAN UJI COBA APLIKASI

4.1 Tampilan Layar *Login*

Form Login akan tampil pada saat aplikasi dijalankan. Pengguna harus mengisi *Username* dan *Password* kemudian klik tombol *Login*, sehingga dapat masuk ke dalam Menu Utama. Bentuk tampilannya sebagai berikut:



Gambar 7.Tampilan layar Login

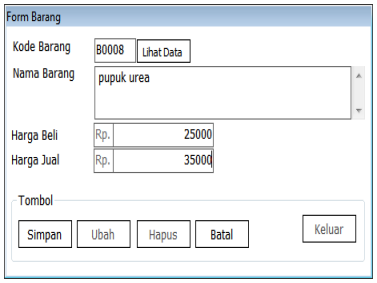
4.2 Tampilan Layar Menu Utama

Tampilan layar menu utama akan muncul ketika pengguna berhasil melakukan *login*. Pada menu utama terdapat 8 Menu yaitu *form* Barang, *form* pelanggan, *form* penjualan, laporan penjualan, *form* pengaturan, tentang, Petunjuk, Keluar Pada Menu *Form* Pengaturan terdapat menu item pengaturan *key* dan item pengaturan *user*. Tampilan layar menu utama dapat dilihat seperti pada Gambar 8 berikut ini:

Gambar 8.Tampilan Menu Utama

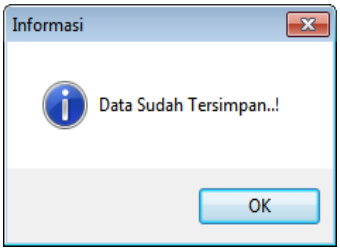
4.3 Form Tampilan Layar Barang

Tampilan Layar *Form* Barang terdapat di tab pojok kanan atas di menu utama. Pada *form* barang terdapat kode barang yang secara otomatis terinput sesuai dengan urutan kode barang, terdapat juga *field* penginputan nama barang, harga beli, dan harga jual. Terdapat 5 *button* yaitu simpan, ubah, hapus, batal, dan keluar dan terdapat 1 *button* yaitu lihat data, seprti gambar 9 berikut ini:



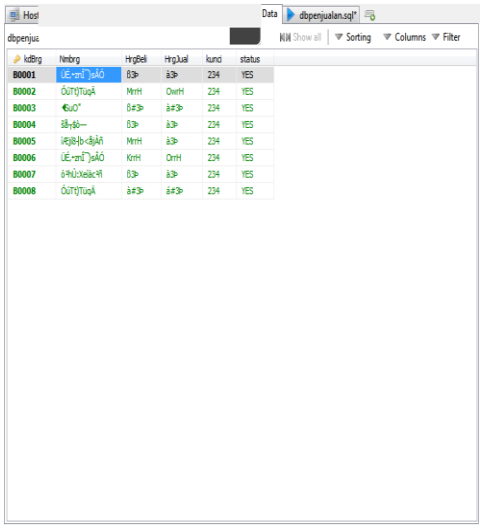
Gambar 9. Layar Form Barang

Semua proses pencarian, penambahan, perubahan, serta penghapusan data yang pada *form* barang akan memunculkan pemberitahuan berbentuk *message* dialog yang dapat dilihat seperti pada gambar 9 sampai gambar 10, Pada Gambar 10 muncul *message* dialog berhasil apabila *user* berhasil menambahkan data barang.



Gambar 10: Tampilan Message Dialog Berhasil Menyimpan Barang

Maka data yg disimpan tadi akan tersimpan di dalam database, berikut adalah tampilan data barang yang disimpan di database.



Gambar 11. Hasil Enkrpsi Data Barang Pada Database

4.4 Evaluasi Program

Evaluasi adalah salah satu hal yang dilakukan dalam setiap pengembangan aplikasi untuk mengetahui kelebihan dan kekurangannya. Dalam evaluasi ini ditemukan beberapa kelebihan dan kekurangannya antara lain :

4.4.1 Kelebihan Program

a) Tampilan aplikasi *user friendly* sehinga mudah digunakan.
b) *Database* penjualan menjadi lebih aman karan telah melakukan proses enkripsi.
c) Hasil *report* penjualan bisa langsung dilihat oleh admin dan dapat melihat langsung menghitung estimasi kebutuhan serta keuntungan.
d) Mempermudah pencarian data pada *database.*

4.4.2 Kekurangan Program

a) Banyaknya data penjualan yang tampil adalah sesuai yang *user input*.
b) Tidak bisa diakses dimana saja karena berbasis desktop.
c) Ukuran *file* enkripsi menjadi lebih besar.

Dari hasil analisis yang telah dilakukan terhadap permasalahan dari aplikasi yang telah dibuat, maka dapat ditarik beberapa kesimpulan dan saran yang mungkin dibutuhkan oleh penulis dikemudian hari.

5. Kesimpulan

Hasil yang telah kami lakukan terhadap analisis permasalahan dalam aplikasi yang dikembangkan dapat disimpulkan sebagai berikut:

5.1 Kesimpulan

a. Enkripsi TCC (*Triangle Chain Cipher*) dapat diimpementasikan pada aplikasi pengamanan *database* dengan menggunakan bahasa *VB.net* dan *database HeidiSQL*.
b. Aplikasi ini dapat mengamankan data yang masuk kedalam *database* dengan teknik kriptografi menggunakan metode TCC (*Triangle Chain Cipher*) sehingga data yang tersimpan kedalam *database* akan sulit untuk dibaca.
c. Aplikasi ini dapat dijalankan sesuai dengan spesifikasi teknik yang dirancang.

5.2 Saran

Selain menarik beberapa kesimpulan, dapat pula diajukan saran-saran yang mungkin bisa dijadikan pertimbangan dalam pengembangan sistem, antara lain:

a. Diharapkan dilakukan pelatihan terlebih dahulu kepada *user* agar *user* benar-benar memahami sistem dan cara penggunaan sekaligus pemeliharaannya sehingga sistem dapat digunakan dengan optimal untuk jangka waktu yang lama.

b. Progam atau perangkat lunak ini dapat dikembagkan dengan menambahkan penjelasan yang lebih detail dan lebih baik.

6. DAFTAR PUSTAKA

[1] Jumrin, Sutardi, & Subardin. (2016). Sistem Keamanan Basis Data menggunakan Teknik Kriptografi RC4 *Stream Cipher*. Jurnal semanTIK, Vol.2, No.1, Jan-Jun 2016, pp. 59-64 ISSN : 2502-8928.

[2] Kromodimoeljo, S. (2009), "Teori dan Aplikasi Kriptografi", Penerbit SPK ITConsulting,Yogyakarta.

[3] Basri. (2016). Kriptografi Simetris dan Asimetris Dalam Pespetif Keamanan Data dan Kompleksitas Komputasi. Jurnal Ilmiah Ilmu Komputer, Vol. 2, No. 2, ISSN 2442-4512, ISSN 2503-3832

[4] Hasrul, & Siregar, H.L. (2016). Penerapan Teknik Kriptografi Pada Database Menggunakan Algoritma *One Time Pad*. Jurnal Elektronik Sistem Informasi dan Komputer, ISSN: 2477-5290, ISSN: 2502-2148. Vol.2 No.2.