KEAMANAN ALGORITMA KRIPTOGRAFI DATABASE MENGGUNAKAN METODE ADVANCED ENCRYPTION STANDARD (AES-128) BERBASIS DESKTOP

Pandu Pradinata[1)], **Muhammad Syafrullah**[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : pandupradinata0995@gmail.com[1)], mohammad.syafrullah@budiluhur.ac.id[2)]

Abstrak

PT. BPR Marcorindo Perdana adalah sebuah perusahaan bank perkreditan rakyat yang bergerak dalam bidang peminjaman uang yang usahanya bergerak di bidang perbankan. PT. BPR Marcorindo Perdana hampir setiap harinya melakukan transaksi. Dengan banyaknya orang yang menggunakan jasa perkreditan diperusahaan tersebut sehingga terjadi persaingan yang tidak sehat dengan perusahaan yang lainnya dan cara apapun dilakukan agar mendapat keuntungan, pencurian data pun dilakukan untuk menjatuhkan nama baik perusahaan itu. Untuk Meminimalisir hal tersebut maka dibuatlah suatu aplikasi pengamanan database berbasis desktop menggunakan algoritma kriptografi (AES-128) *bit*. Perancangan aplikasi tugas akhir ini menggunakan metodologi pengembang SDLC (*Software Development Life Cycle)*. Kriptografi (AES-128) *bit* merupakan algoritma simetris dengan keamanannya sangat *real*, atau bisa dikatagorikan sebagai keamanan yang cukup baik, dengan mempunyai alur proses yaitu memiliki 10 putaran yang dimana dengan proses melakukan enkripsi data yang tidak bisa dibaca dan dekripsinya adalah mengembalikan data asli yang nantinya dapat bisa dibaca. Bahasa pemograman yang digunakan pada aplikasi ini adalah Java dengan editor NetBeans 8.0.2 data yang di input kedalam tabel akan terlebih dahulu di enkrpsi. Untuk melakukan edit dan hapus data dengan melakukan dekripsi terlebih dahulu. Dengan adanya aplikasi ini bertujuan untuk pengamanan data dalam database dengan kriptografi dan penginputan kedalam database sehingga isi dari databse tersebut tidak dapat dimengerti oleh orang lain kecuali oleh orang yang memiliki kunci yang digunakan untuk membuka record.

Kata kunci: Kriptografi, AES 128, Keamanan Database

1. PENDAHULUAN

Dalam kemajuan teknologi yang sangat pesat dan akurat mendorong untuk perusahaan ataupun instansi untuk tetap mengikuti perkembangan teknologi dan informasi semakin pesat yang memudahkan proses pengiriman dan penerimaan data sangat mudah. Namun kemudahan tersebut tidak menjamin data maupun file yang dikirim dapat terjaga keamananya. Untuk itu maka dibutuhkan sebuah sistem aplikasi untuk mengamankan data tersebut.

Penerapan dalam teknologi komputer di Indonesia sudah menjadi kebutuhan penting dalam membantu kelancaran pada setiap kegiatan dari segi pendidikan, ekonomi, dan kegiatan kegiatan lainya. Berbagai data-data maupun informasi sudah semakin mudah dilakukan yang dapat dilakukan tanpa adanya media fisik.informasi atau data tersebut menjadi kurang tepat dan kurang efektif.

Dalam hal ini perkembangan teknologi-teknologi informasi berdampak sangat besar dengan adanya perubahan-perubahan aktifitas pada manusia, tak terkecuali dalam hal penyimpanan data. Selama ini PT. BPR *marcorindo* perdana. mempunyai data Dalam upaya untuk mengatasi permasalahan dalam hal mengamankan data. Salah satu cara untuk mengamankan data dari pihak yang tidak bertanggung jawab adalah sebuah sistem aplikasi pengamanan data dengan menggunakan teknik Kriptografi. Algoitma tersebut adalah suatu ilmu yang mempelajari bagaimana cara menggunakan aplikasi dengan teknik enkripsi dan juga dekripsi agar data atau pesan tetap aman saat dikirim maupun diterima. Algoritma yang digunakan untuk kriptogafi ini adalah AES 128. Algoritma ini merupakan algoritma yang cukup sederhana dan mudah dimengerti.

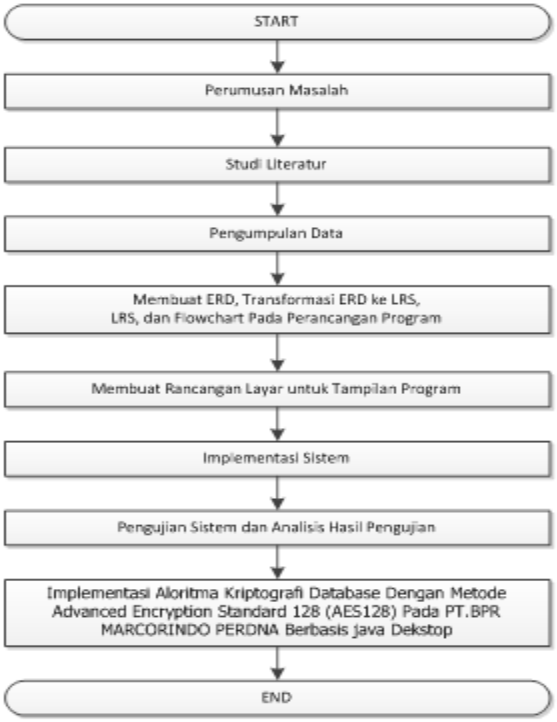
PT. BPR Marcorindo Perdana adalah perusahaan yang bergerak dalam bidang perbankan. Data pada perusahaan ini harus dijaga kerahasiaannya agar tidak terjadi pencurian data. Salah satunya dengan pengamanan kriptografi dengan metode Algoritma AES 128 agar *record database* yang disimpan menjadi aman dan tidak ada yang dapat mengakses dengan mudah.

Kriptografi bertujuan agar data yang diinputkan tidak diketahui oleh orang lain berkaitan dengan hal diatas, maka dilakukan implementasi terhadap pengamanan data atau informasi dengan mengimplementasikan algoritma tersebut kedalam aplikasi sehingga dapat mengamankan data-data yang penting.

2. ANALISA MASALAH DAN RANCANGAN PROGRAM

2.1 Proses Penelitian Program

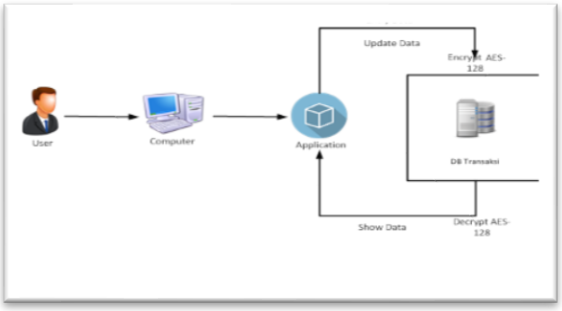
Pada proses penelitian ini dapat menggambarkan alur proses studi literature dengan tahap pengumpulan data dengan mewawancarai dan melakukan proses observasi pada pihak peusahaan tersebut. selanjutnya dengan pengumpulan berita atau adata-data kemudia diolah dengan mengimplementasikan menjadi rancangan *ERD* (Entity Relationship Daiagram). Dengan tahap selanjutnya dengan dengan pengujian system yang telah dirancang serta kejurangan dan kelebihannya dengan menggunakan algoritma kriptografi (AES-128) *bit.* Seperti gambar berikut ini:



Gambar 1. Proses Penelitian Program.

2.2 Arsitektur Program

Pada tampilan arsitektur program ini dapat menggambarkan suatu alur program yang dibuat, dan agar dapat lebih memahami konsep program yang dibuat. Karena program yang dibangun ini adalah sangat penting untuk perusahaan dan leih tepatnya mempunyai kelebihan dan kekurang tersendiri pada program ini. gambar arsitektur pada gambar 3 pada gambar arsitektur sistem menggambarkan secara garis besar proses dari keseluruhan system.



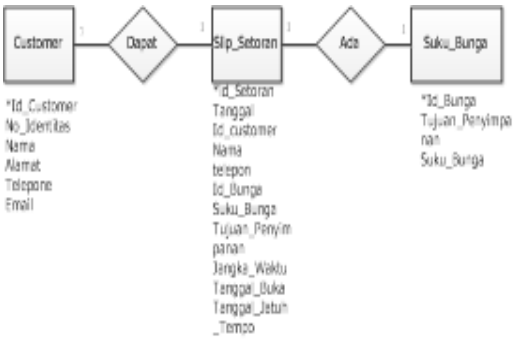
Gambar 2. Arsitektur Aplikasi.

2.3 Rancangan Basis Data

Berikut adalah rancangan basis data yang dibuat, antara lain :

a. *Entity Relationship* Diagram (ERD)

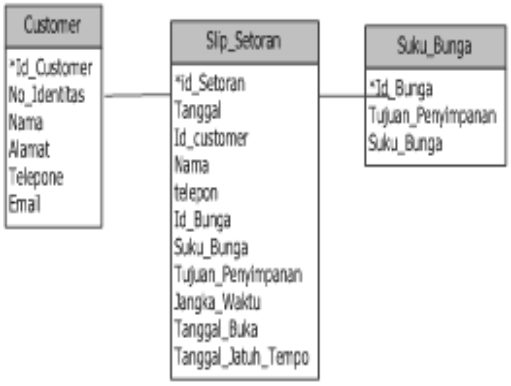
Alur Proses ERD (*Entity Relationship Diagram*).



Gambar 3. Alur Proses *Entity Relationship Diagram* pada Database.

b. Transformasi *Logical Record Structure* (LRS).

Berdasarkan gambaran *LRS* ini adalah proses yang dimana alur menunjukan antara customer, slip_setoran dam suku_bunga masing-masing mempunyai isi agar menunjukan bahwa data data tersebut dapat sesuai dengan alur *primary key* tersebut.



Gambar 4. Alur Proses Transformasi LRS Database.

c. Tabel Basis Data *Login*

Pada spesifikasi tabel basis data *login* adalah untuk proses awal masuk aplikasi, terda[at *username* dan *password* berfungsi untuk awal masuk aplikasi, *user* diperintahkan untuk membuat *username* dan *password* dengan sesuai. Seperti gambar ber

No	Nama *field*	Tipe data	*Length*	Keterangan
1	*username*	Varchar	20	*username* dari login
2	*password*	Varchar	32	*password* dari login

Tabel 1. Tabel Basis Data *Login.*

d. Tabel Basis Data Slip Setoran

Pada spesifikasi tabel basis data slip setoran adalah *user* akan melakukan proses mengisi data slip setoran , bila saat ada customer ingin melakukan transaksi maka *user* melakukan proses buat data dengan ketentuan yaitu slip setoran. Seperti gambar berikut ini:

No	Nama *field*	Tipe data	*Length*	Keterangan
1	id_Setoran	int	11	Id dari Setoran
2	Tanggal	date	500	Tanggal dari
3	id_customer	Varchar	500	Id dari cari customer
4	Name	Varchar	500	Nama customer
5	Telepone	Varchar	500	Telepon customer
6	Id_bunga	Varchar	500	Id dari Id_Bunga
7	suku_bunga	Varchar	500	Suku_Bunga
8	tujuan_penyimpanan	Varchar	500	Tujuan_penyimpanan
9	Jangka_waktu	Varchar	500	Jangka_waktu
10	Tanggal_buka	Varchar	500	Tanggal_buka
11	Tanggal_jatuh_tempo	Varchar	500	Tanggal_jatuh_tempo

Tabel 2. Tabel Basis Data Slip Setoran.

e. Tabel Basis Data *Customer*

Pada spesifikasi tabel basis data *cutomer* adalah *customer* akan melakukan pendaftaran dengan ketetentuan yang tersedia pada data tersebut, dengan meng-*input* sebuah data yang sesuai. Seperti gambar berikut ini:

No		Nama *field*	Tipe data	*Length*	Keterangan
1		Id_customer	Int	6	Id dari customer
2		No. Identitas	Varchar	50	NIK dari customer
3		Nama	Varchar	255	Nama dari customer
4		Telepone	Varchar	15	Telepon dari customer
5		Alamat	Varchar	50	Alamat dari customer
6		Email	Varchar	50	Email dari customer

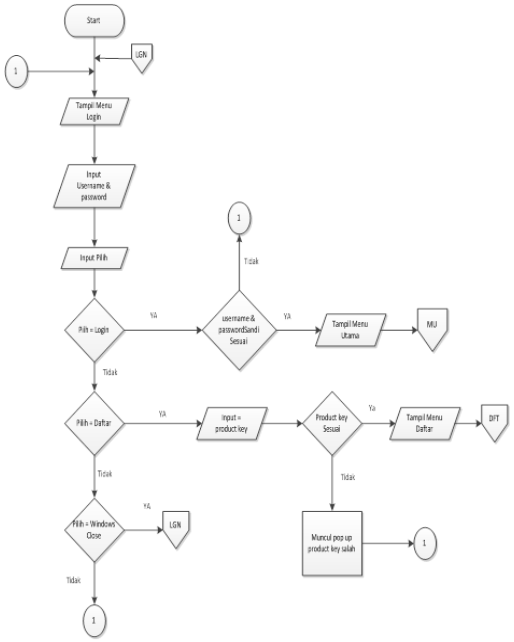
Tabel 3. Tabel Basis Data *Customer*.

2.4 Flowchart

Flowchart adalah suatu bagan dari alur aplikasi yang nantinya akan diimplementasikan secara teratur. Dalam hal ini *flowchart* mempunyai simbol-simbol yang berbeda dan masing-masing simbol tersebut dapat mempunyai arti dan saling berhubungan tergantung alur aplikasi tersebut dengan proses lainya dalam suatu program.

a. Flowchart login

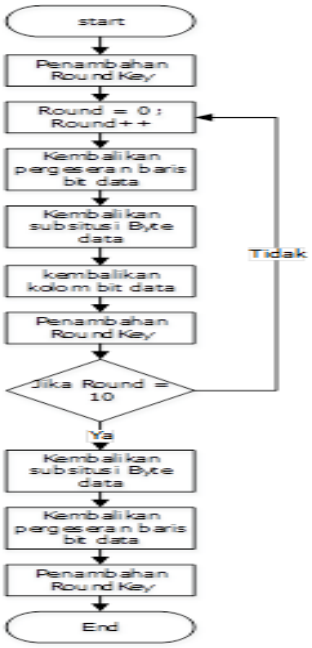
merupakan gambaran alur proses dari *form login*. Form *login* merupakan *form* yang pertama kali muncul saat program dijalankan.



Gambar 5. *Flowchart Login.*

b. Flochart Enkripsi Advanced Encryption Standard (AES-128).

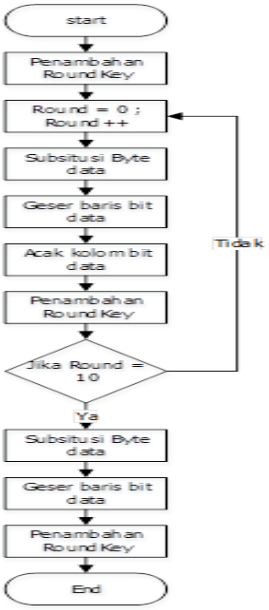
Flowchar ini menjelaskan tentang alur aplikasi tersebut, dan bagaimana proses cara kerja aplikasi tersebut, dengan mengimplementasikan sebuah algoritma kriptografi (AES-128)bit, yang nantinya akan mengekripsi data bisa dikatagorikan data-data perusahaan. Seperti gambar berikut ini:



Gambar 6. *Flowchart Enkrip Standard* (AES-128) *bit.*

c. Flochart Enkripsi Advanced Encryption Standard (AES-128).

Flowchar ini menjelaskan tentang alur aplikasi tersebut, dan bagaimana proses cara kerja aplikasi tersebut, dengan mengimplementasikan sebuah algoritma kriptografi (AES-128)bit, yang nantinya akan mendekripsi data tersebut. Hal ini bisa dikatagorikan menderipsi data perusahaan dengan mengembalikan data asli yaitu data yang telah sudah dienkripsi. Seperti gambar berikut ini:



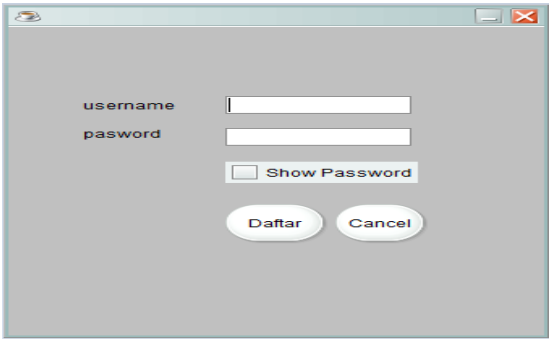
Gambar 7. Flowchart *Advenced Dekripsi Standard (* AES-128) *bit.*

3. HASIL DAN PEMBAHASAAN

3.1 Tampilan Layar Form *Login*

Tampilan Layar pertama yang akan tampil ketika saat aplikasi tersebut proses dijalankan. Pada tampilan form *login* ini terdapat tombol daftar berfungsi untuk proses mendaftar, jika *user* tidak memilik akun maka lakukan proses daftar dengan cara memilih tombol daftar dengan meng-*input username* dan *password* dengan sesuai, jika proses sesuai maka akan proses tampil ke halaman berikutnya. akun hanya bisa dapat digunakan sekali saja. Seperti gambar berikut ini :

Gambar 8. Tampilan Layar Form *Login.*



Gambar 9. Tampilan Layar Form Daftar.

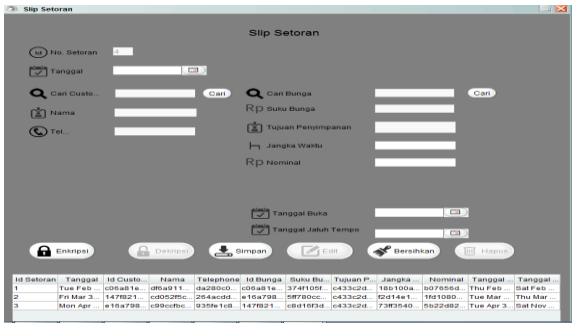
3.2 Tampilan Layar Menu Utama.

Tampilan Layar Menu Utama menggambarkan terdapat Menu bar Master, Menu bar Transaksi Nilai dan Info. Pada Menu *Editor* terdapat Master dengan berisi menu *item* Master Customer, Master Suku Bunga. Dam untuk Menu *Editor* Transaksi terdapat dengan berisi menu *item* Slip Setoran. Pada Menu *Editor* Info terdapat dengan berisi menu *item* Bantuan dan *About*. Seperti gambar berikut ini :

Gambar 10.Tampilan Layar Menu Utama.

3.3 Tampilan Layar Proses Enkripsi Data Transaksi Data Slip Setoran

Tampilan layar enkipsi. Pada proses ini merupakan tampilan layar hasil enkripsi yang sudah tersimpan pada database. Pada form ini yang jadi media untuk diamankan yaitu berupa data dari hasil *entry* data slip setoran, yang dimana data tersebut bersifat renta jika tidak diamankan. Maka dari itu data terbut dapat diamankan dengan mengimplementasikan menggunakan algotima kriptografi AES-128. Hasil enkripsi didapat ketika *user* memasukan data lalu menekan tombol enkipsi lalu data tersebut akan terenkripsi setelah itu *user* dapat mengklik tombol simpan agar data yang sudah terenkripsi tersimpan dalam database yang ditampilkan pada tabel. Seperti pada gambar berikut ini :



Gambar 11. Tampilan Layar Proses Enkripsi Data Transaksi Slip Setoran.

3.4 Tampilan Layar Proses Dekripsi Data Slip Setoran

Tampilan layar hasil dekripsi. Pada proses ini jika *user* ingin melakukan atau mengubah data tersebut menjadi data semula maka langkahh selanjut *user* dapat memilih tombol *decryption.*

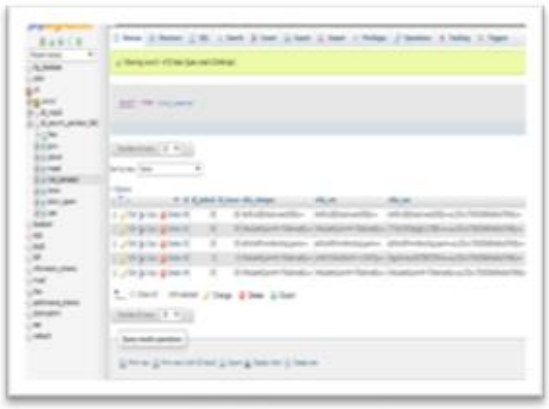
hasil dekripsi didapat ketika *user* menampilkan data hasil enkripsi lalu menekan tombol dekripsi lalu data tersebut akan terdekripsi setelah itu *user* bisa *mengupdate* data setelah data selesai *diupdate user* memiliki pilihan untuk menyimpan data terenkripsi atau tidak jika *user* ingin data yang *diupdate* terenkripsi kembali *user* harus menekan tombol enkripsi untuk mengenkripsi data dan jika *user* tidak ingin mengenkripsi kembali *user* hanya tinggal menekan tombol *edit* agar data yang sudah *diupdate*

Gambar 12. Tampilan Layar Proses Dekripsi Data Transaksi Slip Setoran.

4. UJI COBA APLIKASI

4.1 Tampilan Layar *Encryption* Pada *Database* Nilai.

Tampilan layar *encrypt* data dalam database, yaitu berguna untuk penyimpanan dan pembuktian bahwa data tersebut memang dapat berjalan dengan baik, dan juga untuk penampungan didalam *database* tersebut dapat menampung dengam sesuai, maka dari itu sangat penting. data yang terenkripsi hanya data-data tertentu saja. Seperti gamabar berikut ini:



Gambar 13. Tampilan Layar Enkripsi Data Slip_setoran Untuk *Basis Data*.

4.2 Tabel Pengujian *E*ncryption Data Slip Setoran

Pengujian ini dilakukan untuk mengetahui panjang dari symbol yang dihasilkan dari proses enkripsi-atau dekripsi menggunakan metode *Advanced Encryption Standard* (AES 128) dan menyamakannnya dengan panjang karakter *text* Dikatakan linier jika panjang hasil enkripsi berbeda dengan panjang karakter teks aslinya. Berikut adalah gambar hasil simbol enkripsi *Advanced Encryption Standard* (AES 128) dan untuk lebih jelasnya dapat dilihat pada tabel hasil enkripsi dibawah ini.

Data	Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah karakter Hasil Enkripsi
Id Setoran	2	1	-	-
Tanggal	Januari 4, 2018	11	-	-
Cari Customer	3	1	e16a7984b02e61997df834271521286b	32
Nama	UBAIDILLAH	10	c99ccfbc7ac70ef19ea6a4911e8d7df6	32
Telepon	081255387698	12	935fe1c86b6b70a4e45e3b5c6cf91c0d	32
Cari Bunga	7	1	5feac7da8eab14be535cb2b75d1e6d75	32
Suku Bunga	11	2	374f105f72b7616ae9b23e49a7201a9b	32
Tujuan Penyimpanan	Tabungan	8	c433c2d12eee40db8959d768fb69b543	32
Jangka Waktu	90	7	e0b2eb1fffb09fce919886218bb99cd9	32
Nominal	888888888	1	9ed551482b554e9a328909204bf301e6	32
Tanggal Buka	Januari 26, 2018	11	-	-
Tanggal Jatuh Tempo	Januari 26, 2018	11	-	-

Tabel 4. Tabel Pengujian Hasil Enkripsi *Advanced Encryption Standard* AES-128.

4.3 Tabel Pengujian *Decryption* Data Slip Setoran

Pengujian ini adalah proses *decryption yaitu pada saat user ingin melakukan proses mengembalikan sebuat data-data yan dimana sebelumnya data tersebut ingin diubah menjadi data asli maka lakukan proses dekripsi data tersebut.* Seperti gambar berikut ini:

Data	Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah karakter Hasil Enkripsi
Id Setoran	2	1	-	-
Tanggal	Januari 4, 2018	11	-	-
Cari Customer	3	1	e16a7984b02e61997df834271521286b	32
Nama	UBAIDILLAH	10	c99ccfbc7ac70ef19ea6a4911e8d7df6	32
Telepon	081255387698	12	935fe1c86b6b70a4e45e3b5c6cf91c0d	32
Cari Bunga	7	1	5feac7da8eab14be535cb2b75d1e6d75	32
Suku Bunga	11	2	374f105f72b7616ae9b23e49a7201a9b	32
Tujuan Penyimpanan	Tabungan	8	c433c2d12eee40db8959d768fb69b543	32
Jangka Waktu	90	7	e0b2eb1fffb09fce919886218bb99cd9	32
Nominal	888888888	1	9ed551482b554e9a328909204bf301e6	32
Tanggal Buka	Januari 26, 2018	11	-	-
Tanggal Jatuh Tempo	Januari 26, 2018	11	-	-

Tabel 5. Pengujian Hasil Dekripsi i *Advanced Encyption Standard* AES-128.

5. EVALUASI APLIKASI

Evaluasi adalah bermaksud untuk melakukan proses pengembangan aplikasi, untuk mengetahui bagaimana proses fngsi dan cara pemakaian aplikasi tersebut, Juga proses kelebihan dan kekurangan aplikasi tersebut. Seperti gambar berikut ini:

a. Kelebihan Program

1) Aplikasi ini mampu digunakan karena tampilan yang flexible dan sederhana untuk memudahkan *user* dalam menggunakan aplikasi.
2) Data-data yang telah di*input* akan menjadi aman pada saat melakukan proses menjalankan aplikasi tersebut dengan proses enkripsi pada data-data tersebut. Agar meminimalisir adanya pencurian atau hacker
3) Terdapat pengamanan ganda pada bagian data *user* yang cukup aman.
4) Data-data hasil proses dekripsi tidak mengalami perubahan fisik data tersebut. atau kerusakan dan dapat dibaca kembali oleh pengguna.

b. Kekurangan Program

1) Apabila koneksi internet yang *buffring* akan berdampak sangat tidak baik untuk menjalankan aplikasi tersebut, karena aplikasi tersebut bersifat offline.
2) *Interface* aplikasi masih sangat sederhana
3) Karena menggunakan sebagai pihak ketiga, maka proses sewaktu-waktu pada *login* aplikasi perlu mengaktifkan *software MYSQL* dan *apache server* sebagai penghubung antara aplikasi dengan *databse server*.

6. KESIMPULAN

Berdasarkan hasil riset yang telah kami buat untuk mencari permasalahan pada aplikasi yang dikembangkan, maka kami dapat tertarik suatu kesimpulan sebagai berikut:

a. Dengan adanya aplikasi untuk pengamanan *database* menggunakan algoritma kriptografi (AES-128) *bit.* ini dapat mengamankan data penting atau informasi lainnya seperti slip setoran supaya dapat lebih terjaga keamanannya dan kerahasiaannya data-data perusahaan dari pihak hacker atau orang yang tidak bertanggung jawab.
b. Dengan adanya aplikasi tersebut, dapat memudahkan *user* untuk menyimpan data-data perusahaan ke dalam sisstem *database* yang sudah ter-enkripsi, dengan menggunakan aplikasi berbasis desktop.

c. Aplikasi ini mampu dapat berfungsi dan dipakai oleh perusahaan yang belum mempunyai keamanan dalam data-data tersebut.

7. SARAN

Selain menarik beberapa kesimpulan-kesimpulan dalam hal ini *user* ingin memberi saran tentang aplikasi tersebut dalam pengembangan sistem, antara lain:

a. Program ini dapat proses mengenkripsi data per-*record* pada database.
b. Interface masih sangat sederhana, diharapkan bisa ditambahkan beberapa fitur seperti *progress* bar dan waktu lama proses enkripsi dan dekripsi.
c. Aplikasi ini dapat dikembangkan , jika saat data yang dienkripsi berjumlah banyak kedepannya bisa mengenkripsi per-*tabel*.
d. Dapat lebih difokukan untuk pengamanannya , sehingga data yang telah sudah diamankan dapat tidak bisa dicuri oleh hacker.

8. DAFTAR PUSTAKA

[1] Latif, A., 2015. Implementasi Kriptografi Menggunakan Metode Advanced Encrpytion Standard (AES) untuk pengamanan data teks. Merauke: Jurnal Ilmiah Mustek Anim Ha Vol. 4,No.2: 2089-6697

[2] Haji, W.H., Mulyono, S, 2012. *Implementasi RC4 Stream Cipher Untuk Keamanan*

[3] Kustian, N., 2014. Sistem Informasi Pengamanan Basis Data Menggunakan Teknik Enkripsi Bagian Tata Usaha Lembaga Sandi Negara. Factor Exacta, 7(2), pp.188–199. ISSN: 1979-276X.

[4] Taroniksoki. 2013. *Analisa Dan Implementasi Algoritma Triangle Chain Pada Penyandian Record Database*. Medan: Pelita Informatika Budi Darma, Volume III No.2: 2301-9425

[5] Haryanto H, Wiryadinata R, Afif, M., 2014. Implementasi Kombinasi Algoritma Enkripsi AES 128 Dan Algoritma Kompresi Shannon-Fano., Volume 3, no. 1: 2301-4652

[6] Diffie, Whitfield, Hellman, M.E. 1976. *New Directions in Cryptography*.IEEE Trans. Info. Theory IT-22.

[7] Halik I, Prayudi, Y., 2005. Studi Dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi, Dekripsi Data., SNATI., 6(D), pp.149–158. available ISBN: 979-756-061-6.

[8] Jumrin, Sutardi, Subardin., 2016. Aplikasi Sistem Keamanan Basis Data Dengan Teknik Kriptografi *RC4*., semanTIK, 2(1), pp. 59–64 available ISSN: 2502-8928.

[9] Rizal, Ansar, Suharto. 2011. *Implementasi Algoritma RC4 untuk Keamanan Login Pada Sistem Pembayaran Uang Sekolah*. Dielektrika, ISSN 20869487 Vol. 2 No.2.

[10] Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Penerbit Andi, Yogyakarta.

[11] Wirdasari, Dian. 2008. *Prinsip Kerja Kriptografi dalam Mengamankan Informasi*, Jurnal SAINTIKOM Vol.5 No.2.

[12] Rosyadi A., 2012. Implementasi Algoritma Kriptografi AES Untuk Enkripsi dan Dekripsi Email., Jurnal Trainseint. Vol. 1, no. 3.

[13] Rahmat, Muhammad, Yudi. (2016). Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma *Advanced Encryption Standard* (AES). Jurnal Sisfotek Global Vol. 6 No. 2.

[14] Benni C, Jusuf W, Hermawansyah., 2014. Pengembangan Sistem Keamanan Untuk Toko Online Berbasis Kriptografi AES Menggunakan Bahasa Pemograman PHP dan MYSQL. Jurnal Media Infotama Vol. 11 No. 1.

[15] Fricles A, S. 2013. Perancangan Aplikasi Pengaman Data Dengan Kriptografi *Advanced Encryption Standard* (AES). Jurnal pelita Informatika Budi Darma. Vol IV, No. 1.