APLIKASI PENGAMANAN *DATABASE* KEUANGAN BERBASIS *DESKTOP* MENGGUNAKAN ALGORITMA RC4 DAN *VIGENERE CIPHER*

Jemis Suranta Surbakti[1)], **Subandi**[2)]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : jemissurbakti12345@gmail.com[1)], Subandionline@gmail.com[2)]

Abstrak

PT. Taes Ligatta Teknologi bergerak di bidang Konsultan IT yang memiliki database keuangan. Permasalahan yang diagkat dalam menyelesaikan tugas akhir ini adalah rentannya pencurian atau pengaksesan database keuangan oleh pihak yang tidak berwenang. Tujuan penulisan Tugas Akhir ini adalah Mengamankan table database keuangan di instansi ini. Metode penulisan Tugas Akhir ini terdiri dari pengumpulan data, menganalisa kebutuhan aplikasi, perancangan program, pengkodean, implementasi dan pengujian. Aplikasi enkripsi database berbasis desktop ini dibangun menggunakan bahasa java dan database Mysql-font. Proses pengamanan database dengan menggunakan algoritma Rivest Code 4 (RC4) dan Vigenere Cipher sebagai metode untuk proses enkripsi dan dekripsi pada database perusahaan. Hasil dari penulisan Tugas Akhir ini adalah dengan adanya aplikasi ini diharapkan dapat menjaga kerahasiaan isi dari data, sehingga dapat mengantisipasi terjadinya hal yang tidak diinginkan pada instansi. Berdasarkan hasil analisa serta uji coba menunjukan bahwa aplikasi enkripsi database ini menyatakan bahwa semakin kecil ukuran table database yang diproses, semakin cepat waktu proses enkripsi dan dekripsi jika sebaliknya semakin besar ukuran table database maka semakin lama waktu proses enkripsi dan dekripsi. Juga dapat meminimalisir pencurian data oleh pihak yang tidak bertanggung jawab, dan mampu mengembalikan isi database asli yang telah di enkripsi menjadi seperti semula secara utuh tanpa adanya perubahan.

Kata Kunci: Kriptografi, *Rivest Code 4* (RC4), *Vigenere Cipher*, *Database*, Enkripsi, Dekripsi.

1. PENDAHULUAN

PT. Taes Ligatta Teknologi merupakan suatu perusahaan yang bergerak di bidang Konsultan IT yang memiliki salah satu *database* penting yang berisi data keuangan perusahaan. Sering tabel yang disimpan ke dalam *database* sama hasilnya dengan tulisan yang ditunjukkan sebagai informasi akhir untuk *user*. Tentunya lebih memudahkan orang lain yang tidak memiliki kepentingan untuk dapat melihat dengan mudah isi dari *database* tersebut serta dapat memberi peluang kepada orang tersebut dengan mudah melakukan tindakan pembocoran, mendistribusikan maupun melakukan modifikasi lain pada isi dari *database* tersebut.

Mengamankan data tersebut supaya tidak dapat disalah gunakan diperlukan cara untuk mengatasi masalah-masalah dalam mengamankan data. Salah satu cara yang dapat diimplementasikan untuk mengamankan data yaitu menggunakan teknik kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi, dan anti penyangkalan. Algoritma yang digunakan adalah algoritma RC4 dan Vigenere Cipher yang akan diterapkan pada aplikasi kriptografi berbasis *desktop* untuk mengamankan basis data di PT. Taes Ligatta Teknologi.

Dari uraian diatas, permasalahan yang diangkat dalam menyelesaikan Tugas Akhir ini adalah rentannya pencurian atau pengaksesan pada database keuangan pada PT. Taes Ligatta Teknologi oleh pihak yang tidak berwenang, dan juga belum memiliki sistem keamanan yang baik untuk menghadapi resiko penyerangan data oleh pihak yang tidak berwenang.

Adapun maksud dan tujuan penelitian tugas akhir ini bisa terwujud adalah mengamankan *table database* pada PT. Taes Ligatta Teknologi agar tidak dapat diketahui maupun dimodifikasi oleh pihak yang tidak berwenang, juga dapat mengimplementasikan metode algoritma kriptografi RC4 dan Vigenere Cipher dalam bentuk aplikasi, dan menghasilkan aplikasi pengamanan *table database* berbasis desktop yang baik, mudah untuk dipahami dan dapat digunakan oleh *user*.

2. PENGERTIAN KRIPTOGRAFI, RIVEST CODE 4, DAN VIGENERE CIPHER

2.1. Kriptografi

Algoritma kriptografi disebut juga cipher yaitu aturan untuk enchipering dan dechipering,atau fungsi yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enciphering dan dechipering.[1]

2.2. Rivest Code 4

Algoritma RC4 (Rivest Code 4) Stream Cipher merupakan salah satu algoritma kunci simetris berbentuk stream chipper yang memproses unit atau input data, pesan ataupun informasi. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses atau menambahkan byte tambahan untuk mengenkrip[2].

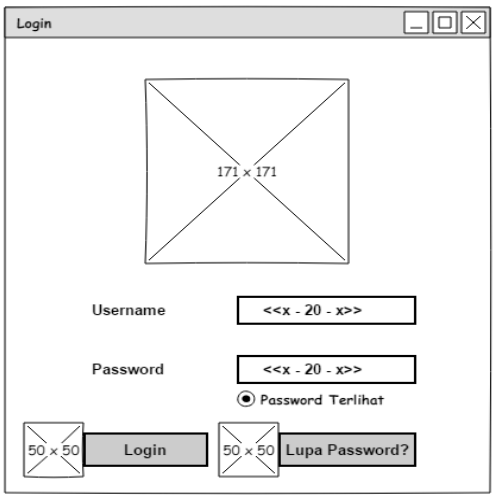
2.3. Vigenere Cipher

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifra del. Sig. Giovan Battista Bellaso pada tahun 1553. Nama vigenere sendiri diambil dari seorang yang bernama Blaise de Vigenere. Nama vigenere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan metode autokey cipher meskipun algoritma dasarnya telah ditemukan lebih dahulu oleh Giovan Battista Bellaso. Algoritmanya adalah Enkripsi : Ci = (Pi + Ki) mod 25Dekripsi: Pi = (Ci – Ki) mod 25 ; untuk Ci > = Ki atau Pi = (Ci + 25 – Ki) mod 25 ; untuk Ci < = Ki[3].

3. ANALISA PERMASALAH DENGAN RANCANGAN PROGRAM

3.1. Rancangan Layar *Form Login*

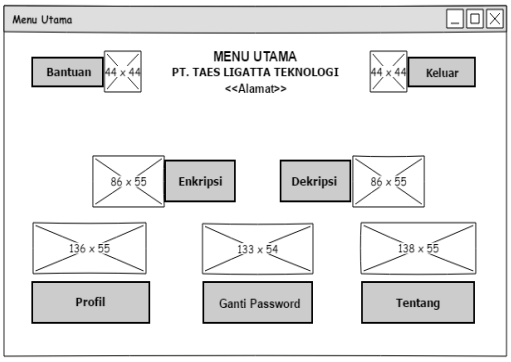
Form Login adalah form yang digunakan *admin* untuk dapat menggunakan aplikasi tersebut. *Form* ini berisikan *Username* dan *Password* yang harus diisi oleh *admin* agar dapat masuk ke dalam sistem. Pada form ini juga terdapat pilihan lupa password.



Gambar 1. Rancangan Layar *Form Login*

3.2. Rancangan Layar Menu Utama

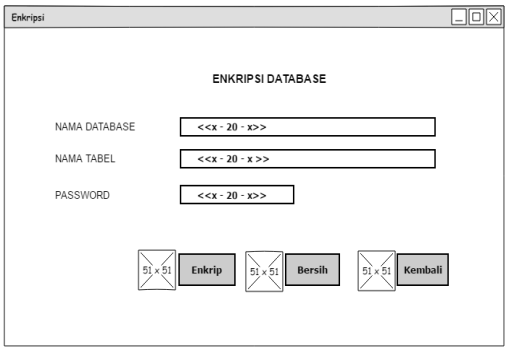
Rancangan layar Menu Utama memiliki 6 menu yaitu, Menu Profil, Menu Enkripsi, Menu Dekripsi, Menu Ganti Password, Menu Bantuan, Menu Tentang.



Gambar 2. Rancangan Layar Menu Utama

3.3. Rancangan Layar *Form* Enkripsi

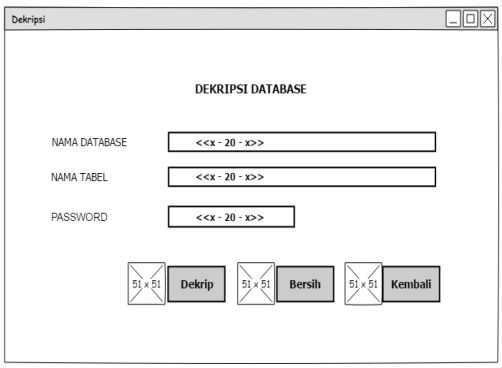
Pada rancangan layar *form* enkripsi, *form* ini berfungsi untuk melakukan enkripsi pada *database* yang akan dieksekusi.



Gambar 3. Rancangan Layar *Form* Enkripsi

3.4. Rancangan Layar *Form* Dekripsi

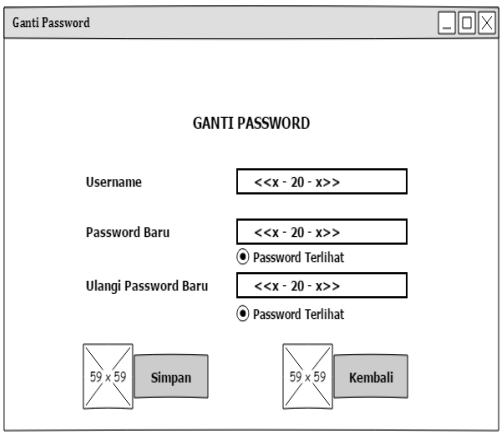
Pada rancangan layar *form* dekripsi, *form* ini berfungsi untuk melakukan dekripsi pada sebuah *database*. Fungsi dari dekripsi ini adalah untuk mengembalikan *database* yang sudah di enkripsi, kembali seperti semula.



Gambar 4. Rancangan Layar *Form* Dekripsi

3.5. Rancangan Layar *Form* Ganti P*assword*

Pada rancangan layar ganti *password*. Menu ganti *password* berguna untuk mengubah *password* secara berkala demi keamanan pribadi.

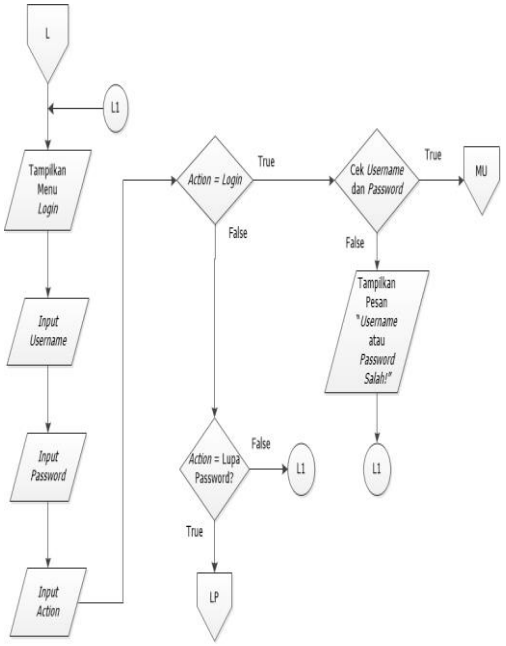


Gambar 5. Rancangan Layar *Form* Ganti *Password*

4. *FLOWCHART*

4.1. *Flowchart Form Login*

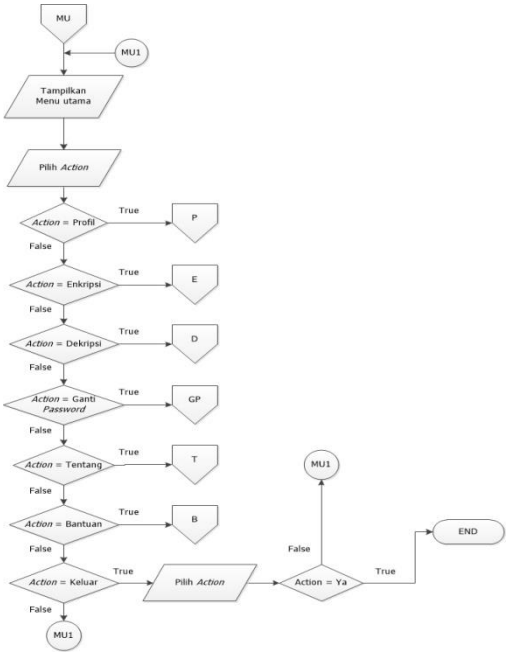
Pada halaman ini terdapat menu *login* yang harus diisi oleh *admin* apabila ingin masuk kedalam menu utama.



Gambar 6. *Flowchart Form Login*

4.2. *Flowchart* Menu Utama

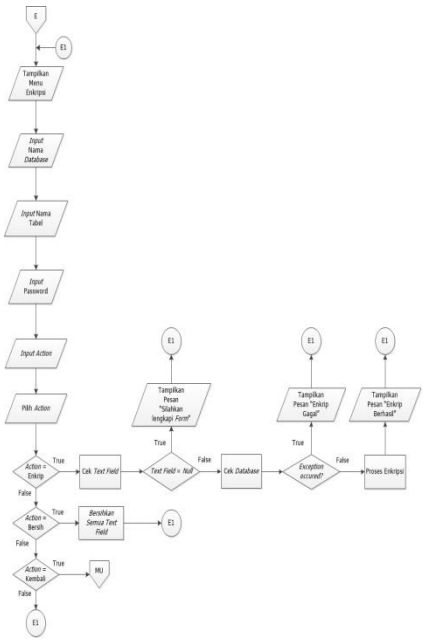
Setelah pengguna login, pengguna akan diarahkan ke halaman Menu Utama. Pada halaman ini terdapat menu yang dapat diakses oleh pengguna sesuai kebutuhannya. Adapun menu yang disediakan adalah menu profil, enkripsi, dekripsi, ganti password, bantuan, tentang dan logout.



Gambar 7. *Flowchart* Menu Utama

4.3. *Flowchart Form* Enkripsi

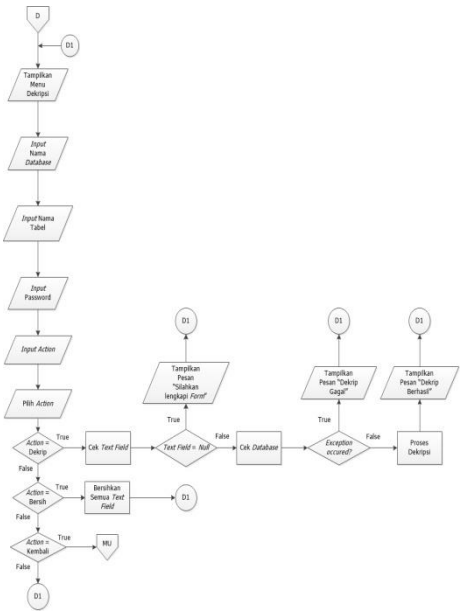
Flowchart form enkripsi merupakan gambaran alur proses dari *form* enkripsi. Pada proses ini pengguna dapat menjalankan proses enkripsi dengan cara memasukan nama *database*, Nama Tabel, dan Password dan setelah itu pengguna memilih tombol enkrip maka proses enkripsi dapat berjalan. Setelah proses enkripsi selesai, pengguna bisa memilih tombol bersih untuk membersihkan nama *database* yang telah di input sebelumnya dan tombol kembali untuk dapat kembali ke Menu Utama.



Gambar 8. *Flowchart Form* Enkripsi

4.4. *Flowchart Form* Dekripsi

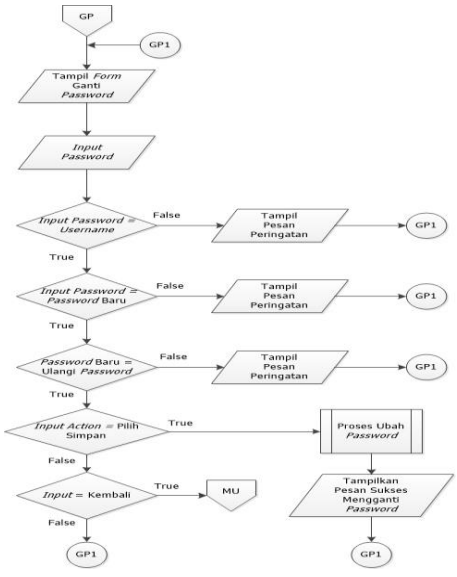
Flowchart form dekripsi merupakan gambaran alur proses dari *form* dekripsi. Pada proses ini pengguna dapat menjalankan proses dekripsi dengan cara memasukan Nama *database*, Nama Tabel, dan Password dan setelah itu pengguna memilih tombol dekrip maka proses dekripsi dapat berjalan. Setelah proses dekripsi selesai, pengguna bisa memilih tombol bersih untuk membersihkan nama *database* yang telah di input sebelumnya dan tombol kembali untuk dapat kembali ke Menu Utama.



Gambar 9. *Flowchart Form* Dekripsi

4.5. *Flowchart Form* Ganti *Password*

Pada halaman ini *admin* diharapkan untuk mengubah password sebelumnya agar tingkat keamanan lebih *user* tersebut lebih terjamin.



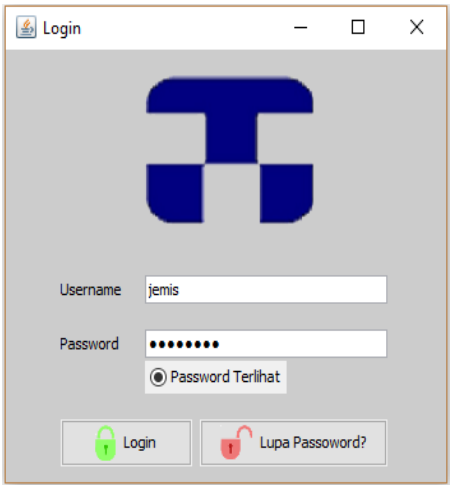
Gambar 10. *Flowchart Form* Ganti *Password*

5. HASIL DAN PEMBAHASAN

5.1. Tampilan Layar *Form* Login

Tampilan layar dari *form Login* pada gambar 11 ini muncul pada pertama kali aplikasi dijalankan yang mengharuskan *admin* memasukan *username* dan *password* yang telah ditentukan

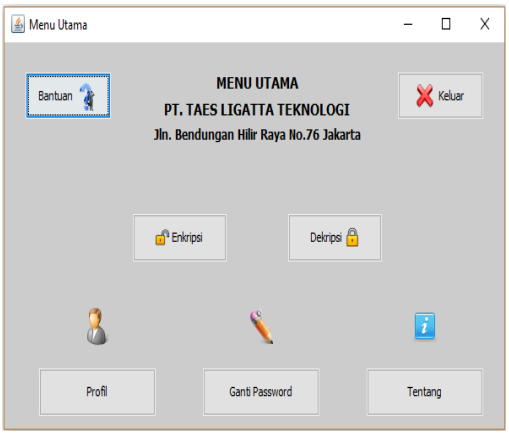
.



Gambar 11. Tampilan Layar *Form Login*

5.2. Tampilan Layar *Form* Menu Utama

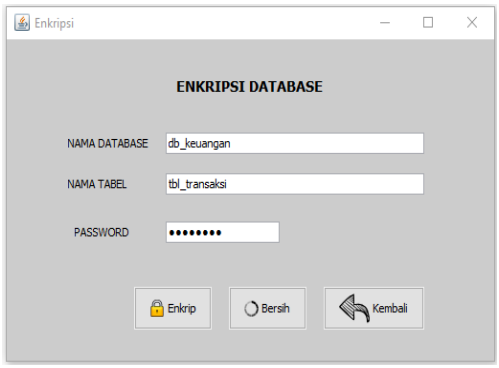
Tampilan layar *Form* Menu Utama pada gambar 12 ini muncul setelah *admin* berhasil *login* ke dalam program, pada *form* ini berisi beberapa menu seperti Enkripsi, Dekripsi, Ganti *Password*, Profil, Tentang, dan Bantuan untuk mempermudah *admin* dalam menjalankan proses enkripsi dan dekripsi.



Gambar 12. Tampilan *Form* Menu Utama

5.3. Tampilan Layar *Form* Enkripsi

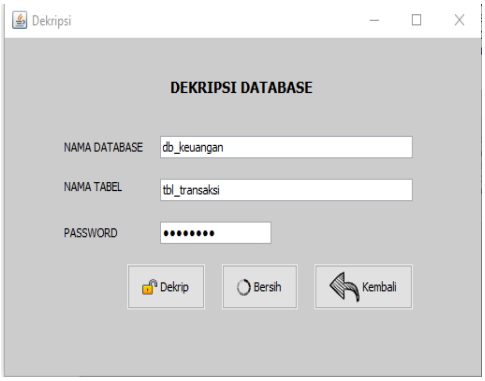
Tampilan layar *form* enkripsi pada gambar 13 berfungsi untuk melakukan enkripsi database. *Admin* terlebih dahulu memasukan nama *database* yang akan dienkripsi, selanjutnya memasukan nama tabel *database* yang akan dienkripsi, dan terakhir isi password yang telah dibuat sebelumnya, lalu dengan mengklik tombol enkrip maka proses enkripsi akan berjalan.



Gambar 13. Tampilan Layar *Form* Enkripsi

5.4. Tampilan Layar *Form* Dekripsi

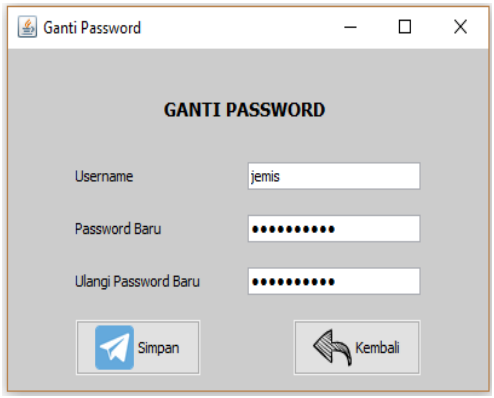
Tampilan layar *form* dekripsi pada gambar 14 berfungsi untuk melakukan dekripsi database. *Admin* terlebih dahulu memasukan nama *database* yang akan dienkripsi, selanjutnya memasukan nama tabel *database* yang akan dienkripsi, dan terakhir isi password yang telah dibuat sebelumnya, lalu dengan mengklik tombol dekrip maka proses dekripsi akan berjalan.



Gambar 14. Tampilan Layar *Form* Dekripsi

5.5. Tampilan Layar *Form* Ganti *Password*

Tampilan layar *form* ganti *password* pada gambar 15 berfungsi untuk mengganti *password* . *Admin* terlebih dahulu memasukan *username*, memasukkan *password* baru, dan memasukkan kembali ulangi *password* baru



Gambar 15. Tampilan Layar *Form* Ganti *Password*

6. Tabel Pengujian

Dalam tahap pengujian kali ini akan dibahas perbandingan pada proses enkripsi dan dekripsi. Pengujiannya meliputi ukuran awal *tabel database* sebelum dienkripsi dan sesudah didekripsi, serta waktu proses enkripsi dan dekripsi.

6.1. Tabel Hasil Pengujian Proses Enkripsi :

Tabel 3, Tabel db_keuangan proses enkripsi

Nama Database	Nama Tabel	Ukuran Size (Byte)	Enkripsi	
			Ukuran (byte)	Waktu (milidetik)
Db_keuangan	Tbl_transaksi	16.384 b	16.384 b	2.255 ms
Db_keuangan	Tbl_user	16.384 b	16.384 b	2.397 ms
Db_keuangan	Tbl_akun	49.152 b	163.840 b	7.928 ms
Rata- rata		81.920 b	196.608 b	12.58 ms

6.2. Tabel Hasil Pengujian Proses Dekripsi :

Tabel 4, Tabel db_keuangan proses dekripsi

Nama Database	Nama Tabel	Ukuran Size (Byte)	Dekripsi	
			Ukuran (byte)	Waktu (milidetik)
Db_keuangan	Tbl_transaksi	16.384 b	16.384 b	2.466 ms
Db_keuangan	Tbl_user	16.384 b	16.384 b	2.717 ms
Db_keuangan	Tbl_akun	163.840 b	49.152 b	8.551 ms
Rata- rata		196.608 b	81.920 b	13.734 ms

7. Evaluasi Program

Berdasarkan pengujian program untuk proses enkripsi dan dekripsi yang telah dibuat, ditemukannya adapun beberapa kelebihan dari aplikasi yang dibuat seperti aplikasi memiliki tampilan yang mudah digunakan oleh *user*, terdapat autentikasi *Username* dan *Password* pada menu *Login*, *database* yang sudah dienkripsi tidak bisa dibaca, isi *database* hasil dari proses dekripsi tidak mengalami perubahan dan, aplikasi memiliki panduan penggunaan proses enkripsi dan dekripsi.

Pada aplikasi ini adapun beberapa kekurangan seperti, diperlukan user yang paham isi *database* agar lebih mudah pada saat menjalankan aplikasi, semakin besar ukuran tabel pada *database* maka akan semakin lama proses enkripsi dan dekripsi, aplikasi hanya dapat melihat hasil enkripsi maupun dekripsi melalui tools database, aplikasi hanya dapat mengenkripsi satu tabel pada satu *database* dalam sekali proses, dan aplikasi hanya dapat mengenkripsi per tabel *database*.

8. KESIMPULAN

Melalui proses perancangan, pembuatan dan pengujian dalam laporan Tugas Akhir ini dapat disimpulkan beberapa hal, diantaranya, aplikasi ini berfungsi merubah *database* asli (*plaintext*) menjadi karakter acak dan tidak dapat dimengerti (*ciphertext*), aplikasi ini mampu mengembalikan isi *database* asli yang telah di enkripsi kembali menjadi data awal tanpa adanya perubahan pada *database.*

Waktu yang diperlukan untuk proses enkripsi dan dekripsi berbanding lurus dengan ukuran *table database* yang diproses (semakin kecil ukuran setiap *table database* yang akan diproses, maka tentunya semakin cepat waktu proses enkripsi dan dekripsi), lalu sebaliknya (semakin besar ukuran *table database* yang akan diproses, maka semakin lama waktu proses enkripsi dan dekripsi).

Dengan menggunakan metode algoritma kriptografi Rivest Code 4 (RC4) dan algoritma Vigenere cipher dapat meningkatkan keamanan *database* yang bersifat rahasia sehingga dapat meminimalisir tingkat pencurian data perusahaan.

9. DAFTAR PUSTAKA

[1] Abdul Halim Hasugian. 2013. Implementasi Algoritma Hill Cipher Dalam Penyandian Data. Pelita Informatika Budi Darma. Medan.

[2] Jumrin, Sutardi and Subardin (2016) 'Aplikasi sistem keamanan basis data dengan teknik kriptografi rc4', *semanTIK*, 2(1), pp. 59–64..

[3] Priyono. (2016) 'Diterbitkan Oleh : Jurnal Riset Komputer (JURIKOM). *Penerapan Algoritma Caesar Cipher dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks*. STIMIK Budi Darma. Medan.