IMPLEMENTASI KEAMANAN DATABASE MENGGUNAKAN ALGORITMA VIGENERE CIPHER DAN RIVEST SHAMIR ADLEMAN (RSA) BERBASIS DESKTOP

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

Abstrak

Seiring dengan perkembangan teknologi dan komunikasi yang begitu pesat, maka kita mudah dan cepat untuk mengirim, menerima dan bertukar informasi melalui media elektronik. Sehingga keamanan suatu informasi telah menjadi hal penting dalam era teknologi saat ini. Aplikasi hanya dapat mengamankan database per record agar tidak dapat diketahui dan dimodifikasi oleh pihak yang tidak berwenang. Algoritma Vigenere Chiper merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi. Sedangkan Algoritma Rivest Shamir Adleman (RSA) termasuk dalam algoritma kriptografi asimetris yang mempunyai dua kunci, yaitu kunci publik (public key) dan kunci pribadi (private key). Dengan dibuatnya aplikasi ini keamanan database ini dapat mengurangi tingkat pencurian data. Uji coba yang dilakukan dengan membandingkan isi database yang telah dienkrip hasilnya isi database yang telah dienkrip teracak. Kemudian uji coba kedua mengembalikan isi database ke bentuk aslinya, hasilnya isi database kembali normal. Kedua uji coba tersebut berhasil dengan proses enkripsi dan dekripsi sehingga isi database tidak mengalami perubahan. Setelah melewati tahap pembuatan dan pengujian program, dapat disimpulkan Proses enkripsi dan dekripsi yang dilakukan pada database berhasil dilakukan dan aplikasi pengamanan database ini dapat berhasil dijalankan sesuai dengan spesifikasi yang telah dirancang.

Kata kunci: RSA, *Vigenere Cipher*, Kriptografi, *Database*.

1. PENDAHULUAN

Seiring dengan perkembangan teknologi dan komunikasi yang begitu pesat, Semakin tinggi teknologi komputer, maka kita mudah dan cepat untuk mengirim, menerima dan bertukar informasi melalui media elektronik. Namun dibalik mudah dan cepat bertukar informasi ditambah semakin tingginyanya teknologi komputer yang digunakan, maka semakin tinggi juga tingkat ancaman yang akan mengancam komputer beserta informasi yang terdapat didalamnya. Terkadang kita juga lengah dengan aspek keamanan data yang akan digunakan atau disimpan sehingga secara tidak langsung menimbulkan celah untuk pencurian data yang kerap kali terjadi. Pencurian data atau informasi merupakan salah satu perkembangan negatif dalam pertukaran informasi dan merupakan salah satu masalah yang ditakuti oleh kita. Dengan adanya pencurian data maka sisi keamanan dalam pertukaran informasi dan penyimpanan data dianggap penting.

Kriptografi merupakan teknik pengamanan informasi, dimana informasi diubah dengan kunci tertentu melalui proses enkripsi sehingga menjadi bentuk informasi baru yang tidak dapat dipahami oleh orang yang tidak berhak. Informasi baru ini hanya dapat diubah menjadi pesan aslinya oleh orang yang berhak melalui proses dekripsi. Data/ informasi tersebut harus tetap rahasia selama disimpan dan harus tetap terjaga kerahasiannya. Dalam penelitian ini algoritma yang akan digunakan adalah algoritma *Vigenere Cipher* dan algoritma RSA(*Rivest Shamir Adleman).*

Untuk dapat menerapkan keamanan tersebut penulis menggunakan bahasa pemrograman *Java (NetBean)* dengan menerapkan proses enkripsi (mengubah bentuk asli kedalam bentuk yang tidak dapat dimengerti) dan proses dekripsi (untuk mengubah kembali kedalam bentuk asli). Algoritma yang digunakan oleh penulis adalah *Vigenere Cipher* dan RSA (*Rivest Shamir Adleman*). Sehingga data yang di enkripsi mempunyai kemungkinan kecil mengalami pencurian data.

2. METODE PENELITIAN

Pada Jurnal ini penulis menggunakan beberapa metode untuk memperoleh informasi yang di perlukan dan menyelesaikan masalah yang ditemui. Adapun metode-metode sebagai berikut :

a. Studi Literatur
   Metode ini menggunakan pembelajaran untuk mengumpulkan, membaca dan memahami jurnal, makalah serta refrensi lain untuk mendapatkan informasi guna menunjang dalam penelitian.
b. Analisis Data
   Menganalisis Algoritma yang digunakan yaitu algoritma Vigenere Cipher dan RSA (Rivest Shamir Adleman), serta teknik-teknik yang digunakan..
c. Perancangan Data
   Merancang system aplikasi untuk mengimplementasikan algoritma Vigenere Cipher dan RSA (Rivest Shamir Adleman) dengan menggunakan bahasa pemrograman java dengan berbasis desktop.

d. Pengujian Sistem
   Metode ini dilakukan dengan cara uji coba jalannya program. Implementasi berdasarkan analisa masalah.

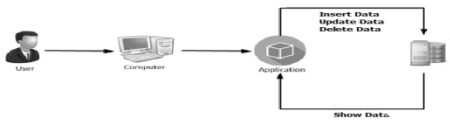
3. Analisis Masalah Dan Perancangan Program

Seiring majunyas teknologi, banyak sekali orang yang dapat mengakses data dan informasi dengan sangat mudah, baik yang bersifat umum maupun yang tidak umum. Hal ini dapat menimbulkan masalah yang baru, terutama masalah pada pengamanan data yang akan masuk kedalam database yang berupa data Transaksi yang data dan informasinya merupakan hal yang tidak dapat diketahui oleh umum.

Dari permasalahan diatas, diperlukannya sebuah aplikasi yang dapat menjaga kerahasiaan data. Pada saat data disimpan ke dalam database. Sehingga isi dari data atau informasi tersebut tidak bisa dapat dilihat atau dibaca oleh orang yang tidak berkepentingan atau tidak berhak melihat atau membaca isi dari data tersebut.

3.1. Arsitektur Sistem

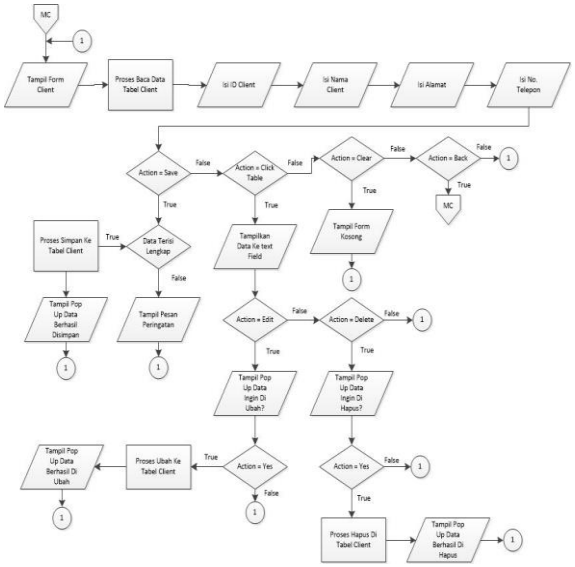
Berikut ini merupakan arsitektur aplikasi, untuk memahami konsep pada aplikasi yang akan dibuat dapat melihat pada gambar 1. Pada gambar arsitektur aplikasi secara garis besar proses dari keseluruhan sistem pada aplikasi.



Gambar 1: Arsitektur Sistem

3.2. *Flowchart Menu Client*

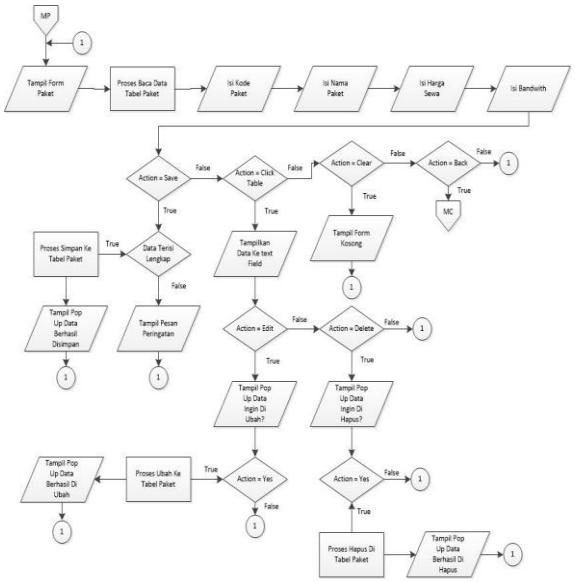
Flowchart ini menjelaskan proses tampilan halaman Menu Client berfungsi menginput, mengubah, menghapus data Client. Seperti gambar 2 berikut ini :



Gambar 2: Flowchart Client

3.3. *Flowchart Menu* Paket

Flowchart ini menjelaskan proses tampilan halaman Menu Paket. berfungsi menginput, mengubah, menghapus data transaksi. Seperti gambar 3 berikut ini :

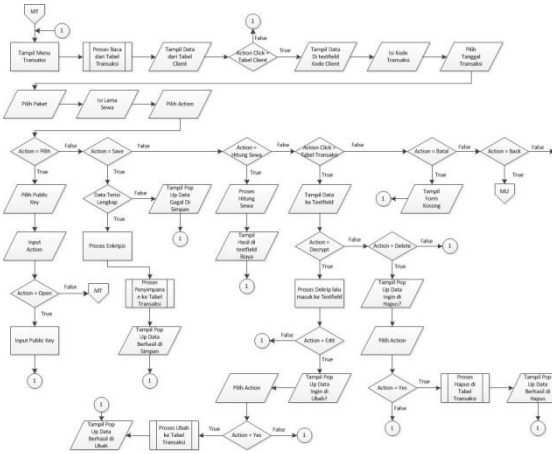


Gambar 3: Flowchart Paket

3.4. *Flowchart Menu* Transaksi

Flowchart ini menjelaskan proses tampilan halaman. Menu Transaksi berfungsi menginput,

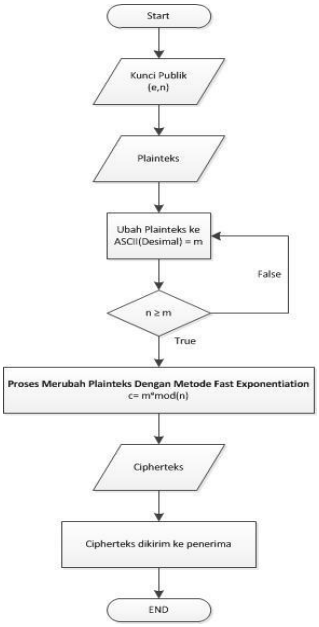
mengubah, menghapus data transaksi. Seperti gambar 4 berikut ini :



Gambar 4: Flowchart Transaksi

3.5. *Flowchart* Enkripsi RSA

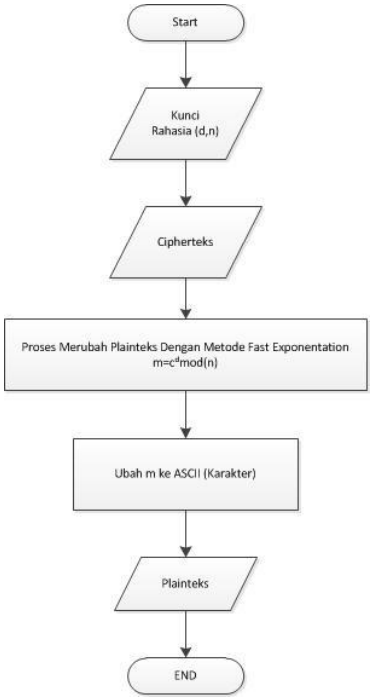
Flowchart proses enkripsi RSA merupakan gambaran alur yang akan mengalami proses enkripsi Seperti gambar 5 berikut ini :



Gambar 5: Flowchart Enkripsi RSA

3.6. *Flowchart* Dekripsi RSA

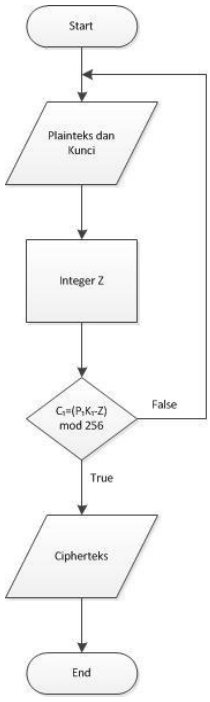
Flowchart proses dekripsi RSA merupakan gambaran alur yang akan mengalami proses dekripsi Seperti gambar 6 berikut ini



Gambar 6: Flowchart Deskripsi RSA

3.7. *Flowchart* Enkripsi Vigenere Cipher

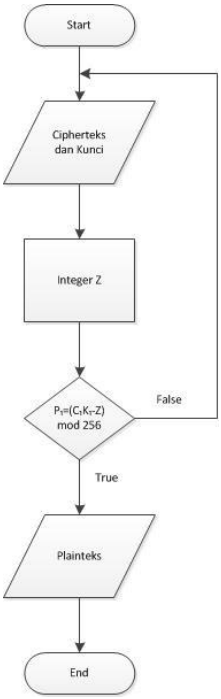
Flowchart proses *enkripsi Vigenere Cipher* merupakan gambaran alur yang akan mengalami proses enkripsi Seperti gambar 7 berikut ini :



Gambar 7: Flowchart Enkripsi Vigenere Cipher

3.8. *Flowchart* Deskripsi Vigenere *Cipher*

Flowchart proses dekripsi *vigenere cipher* merupakan gambaran alur yang akan mengalami proses dekripsi Seperti gambar 8 berikut ini :



Gambar 8: Flowchart Deskripsi Vigenere Cipher

4. HASIL DAN PEMBAHASAN

a. Tampilan Menu Generate Key

Tampilan ini muncul ketika user memilih Menu Generate Key, Menu Generate Key Tampilan layar Generate Key dapat dilihat pada gambar 9 berikut ini:

Gambar 9: Tampilan Menu Generate Key

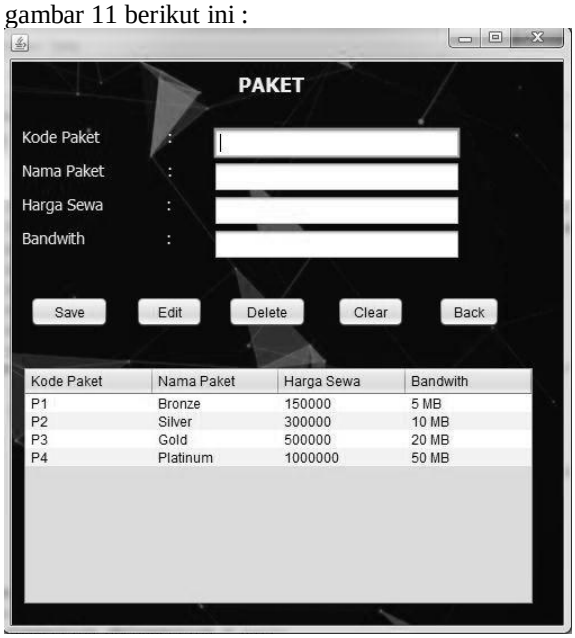
b. Tampilan Menu Client

Tampilan ini akan muncul ketika user memilih Menu Client, Menu Client berfungsi untuk menginput, mengubah, menghapus ataupun melihat data Client.. Tampilan Menu Client dapat dilihat pada gambar 10 berikut ini :

Gambar 10: Tampilan Menu Client

c. Tampilan Menu Paket

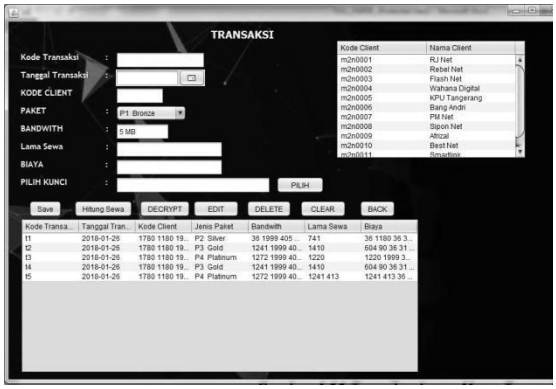
Tampilan ini muncul ketika user memilih Menu Paket, Menu Paket berfungsi untuk menginput, mengubah, menghapus ataupun melihat data Paket. Tampilan Menu Paket dapat dilihat pada gambar 11 berikut ini :



Gambar 11: Tampilan Menu Paket

d. Tampilan Hasil Enkripsi *Menu Transaksi*

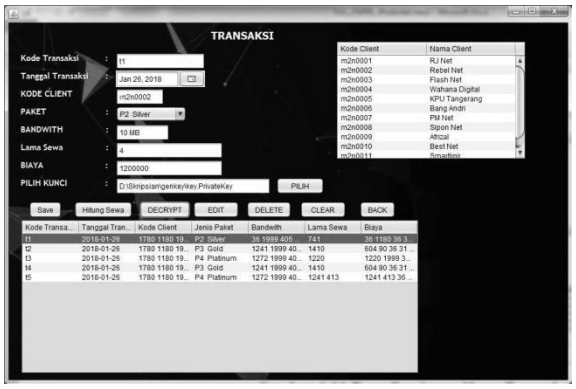
Ini adalah hasil enkripsi menu transaksi. Tampilan layar Hasil Enkripsi dapat dilihat pada gambar 12 berikut ini :



Gambar 12: Tampilan Hasil Enkripsi Menu Transaksi

e. Tampilan Hasil Dekripsi Menu Transaksi

Ini adalah hasil Dekripsi menu transaksi. Tampilan layar Hasil Dekripsi dapat dilihat pada gambar 13 berikut ini :



Gambar 13: Tampilan Hasil Dekripsi Menu Transaksi

f. Tabel Pengujian

Pengujian ini dilakukan untuk mengetahui panjang dari simbol yang didapatkan dari proses enkripsi dan dekripsi menggunakan metode Vigenere Cipher dan Rivest Shamir Adleman(RSA) membandingkannya dengan panjang teks aslinya.

Nama Data	**Karakter Asli**	**Jumlah**	**Karakter Hasil Enkripsi**	**Jumlah Karakter Hasil Enkripsi**
kd_transaksi	t1	2	-	-
tgl_trans	Jan,10,2018	11	-	-
kode_client	m2n0002	7	161 1937 1742 1001 541 1001 1937 1116 147 604 1184 1116 1120 1116 1754 2044 2093 1937	85
jenis_paket	P2 Silver	8	-	-
bandwith	10 MB	5	2093 372 1754 1989 1667 1116 147 604 1184 1116 1120 1116 1754 2044 2093 1937	76
lama_sewa	10	2	2093 372 1116 147 604 1184 1116 1120 1116 1754 2044 2093 1937	61
Biaya	3000000	7	2068 372 2204 1001 541 1001 372 1116 147 604 1184 1116 1120	84

			1116 1754 2044 2093 1937	

Tabel 1 : Tabel Pengujian

Berdasarkan pengujian yang dilakukan penulis, maka didapatkan beberapa hasil uji coba enkripsi seperti pada field kode_client yang memiliki karakter asli "m2n0002" dengan jumlah karakter 7 yang menghasilkan hasil enkripsi "161 1937 1742 1001 541 1001 1937 1116 147 604 1184 1116 1120 1116 1754 2044 2093 1937" dengan jumlah karakter hasil enkripsi sebanyak 85. Jadi dapat ditarik kesimpulan bahwa karakter asli jika di enkripsi maka jumlah karakter hasil enkripsi bertambah 38 %.

5. KESIMPULAN

Kesimpulan yang diperoleh setelah melewati tahap perancangan, pembuatan, serangkaian analisa dan uji coba program aplikasi kriptografi ini, maka dapat disimpulkan sebagai berikut.

a. Proses enkrip dan dekrip ini dilakukan pada database. Database yang asli dapat di enkrip menjadi database yang dirahasiakan dalam bentuk simbol dan dapat di dekrip kembali menjadi database semula sebelum di enkripsi.
b. Aplikasi ini sangat bermanfaat untuk mengamankan *database* agar isinya tidak dapat diketahui, dicuri atau ditiru oleh orang lain yang tidak berhak.
c. Aplikasi ini dapat dijalankan sesuai dengan rancangan yang sudah dibuat sebelumnya oleh penulis.

6. DAFTAR PUSTAKA

[1] Ariyus, Doni. 2008. Pengantar Ilmu Kriptografi (Teori, Analisis, dan Implementasi). Yogyakarta : Andi.

[2] Chandra. Wico.2010, *Kriptografi Dan Algoritma RSA*, Bandung : Institut Teknologi Bandung. Makalah II2092 Probabilitas dan Statistik.