APLIKASI PENGAMANAN TABLE DATABASE MENGGUNAKAN ALGORITMA RIVEST SHAMIR ADLEMAN BERBASIS DESKTOP

Habibi[1)], Subandi, M.Kom[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : habibikd@gmail.com[1)], subandionline@gmail.com[2)]

Abstrak

Sering kali keamanan pada sebuah database disepelekan, dikarenakan keamanan menjadi hal yang kesekian dibandingkan yang lain, namun pada kenyataannya saat ini jika sebuah database diabaikan keamanannya akan menimbulkan kerugian yang besar baik untuk database pribadi, organisasi, lembaga, dan perusahaan. Salah satu cara untuk mengamankan database adalah menggunakan kriptografi, kriptografi adalah teknik pengamanan data yang dilakukan dengan carra mengoIah informasi awal (plaintext) menggunakan suatu kunci tertentu dengan suatu metode enkripsi tertentu hingga menghasilkan suatu informasi yang baru (ciphertext) yang tidak dapat dibaca secara langsung. Algoritma kriptografi yang digunakan penulis adalah algoritma RSA. Algoritma RSA merupakan salah satu algritma public key yang populer dipakai. Kekuatan algoritma ini terletak pada proses eksponensial, dan pemfaktoran bilangan menjadi 2 bilangan prima yang hingga kini perlu waktu yang lama untuk melakukan pemfaktorannya. Bahasa Pemrograman yang digunakan dalam pembuatan aplikasi ini adalah Java Berbasi Desktop. Dengan hadirnya aplikasi ini, kemanan pada database menjadi lebih aman, sehingga kerahasiaannya tetap terjaga. Setelah proses enkripsi sudah dilakukan akan mengeluarkan output yang tentunya tidak bisa di baca atau tidak bisa digunakan oleh pihak yang tidak bertanggung jawab. Proses encrypt dan decrypt yang dilakukan pada database berhasil dilakukan. Database asli dapat dienkripsi menjadi database yang disandikan dan dapat didekripsi menjadi database asli kembali.

Kata kunci: RSA (*Rivest Shamir Adleman*), Kriptografi, *Database*, Enkripsi, Dekripsi, Asimetris, *Java*, *Dekstop*, *Key.*

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Database atau basis data adalah suatu kumpulan data yang disimpan secara teratur pada komputer yang dapat diolah maupun dimanipulasi menggunakan perangkat lunak (*software*) agar dapat menghasilkan informasi. Pendefinisian database meliputi spesifikasi berupa : struktur, tipedata, dan juga batasan-batasan data yang akan disimpan.

Untuk mengakses database pengguna harus terhubung dengan jaringan komputer. Terhubungnya jaringan komputer membuka celah keamanan bagi database tersebut, seperti ancaman sniffing dan sebagainya. Banyak database yang bersifat rahasia dan tidak boleh dirubah oleh pihak yang tidak berkepentingan. Menggunakan kriptografi adalah suatu cara untuk melindungi database dari ancaman.

Salah satu cara untuk mengamankan data pada basis data adalah dengan menggunakan kriptografi. Algoritma kriptografi yang digunakan dalam jurnal ini adalah algoritma RSA (Rivest Shamir Adleman). Algoritma RSA dipilih karena dianggap cepat dalam hal enkripsi, sehingga data yang telah di enkripsi mempunyai tingkat keamanan tinggi terhadap pencurian data. Algoritma RSA termasuk dalam algoritma kriptografi asimetris yang mempunyai dua kunci.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, maka dihasilkan rumusan masalah sebagai berikut :

1) Bagaimana proses enkripsi dan dekripsi data pada table *database*?
2) Bagaimana penerapan Algoritma RSA (Rivest Shamir Adleman) ?
3) Bagaimana merancang sebuah aplikasi kriptografi *database* menggunakan Algoritma RSA (Rivest Shamir Adleman)

1.3 Batasan Masalah

Dalam proses perancangan aplikasi ini, penulis membatasi permasalahan yang akan dibahas, diantar anya adalah :

1) Aplikasi yang dibangun hanya melakukan proses enkripsi dan dekripsi pada table database.
2) Menggunakan Algoritma RSA (Rivest Shamir Adleman)
3) Menggunakan bahasa pemrograman Java.
4) Aplikasi ini hanya digunakan untuk proses enkrip dan dekrip tabel *database.*

1.4 Tujuan Penelitian

Adapun tujuan yang diperoleh dari hasil peneliti an yang dilakukan diantaranya adalah :

1) Mengamankan sebuah data dalam bentuk *table database* agar tidak bisa dibaca oleh orang lain selain pemilik database.
2) Mengimplementasikan algoritma RSA dalam penyandian data.

2. LANDASAN TEORI

2.1. Kriptografi

Algoritma Kriptografi yang baik tidak selalu harus ditentukan oleh rumitnya proses dalam mengolah data atau pesan yang ingin disampaikan. Intinya, algoritma tersebut harus memenuhi 4 Persyaratan berikut :

1. Kerahasiaan.
2. Autentikasi
3. Integritas
4. Non-Repudiation

2.2 Algoritma RSA

Algoritma RSA adalah satu dari sekian algoritma klasik yang masih dipakai hingga sekarang. Kekuatan algoritma ini terletak pada proses eksponensial, dan pemfaktoran bilangan menjadi 2 bilangan prima yang sampai saat ini membutuhkan waktu yang lama untuk melakukan pemfaktorannya.

Algoritma ini dinamakan sesuai dengan nama penemunya, Yaitu : Ron Rivest, Adi Shamir dan Adleman(Rivest-Shamir-Adleman).

2.3 Algoritma Pembangkitan Kunci

Untuk pembangkitan sepasang kunci RSA, digunakan algoritma sebagai berikut:

1) Pilih 2 (dua) bilangan prima acak (sembarang) yang besar p dan q. Nilai p dan q bersifat rahasia.
2) Hitung n = p * q. Besarnya n tidak perlu dirahasiakan.
3) Hitung m = (p-1)(q-1)
4) Pilih e (kunci publik) yang relatif prima terhadap m.
5) Relatif prima terhadap m artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut dengan gcd (e,m) = 1.
6) Hitung d (Private Key), untuk mencari nilai d secara matematis (d * e) mod n = 1.

   Maka hasil dari algoritma tersebut diperoleh:

   1) Kunci publik adalah pasagan (e,n).
   2) Kunci pribadi adalah pasangan (d,n).

2.4 Algoritma Enkripsi Pesan

Untuk enkripsi pesan, digunakan algoritma sebagai berikut :

1) Memakai kunci public (public key) (e,n)
2) Plaintext M dipecah menjadi blok-blok m1, m2, m3, dan seterusnya…
3) Setiap blok mi di enkripsikan menjadi blok ci, dengan rumus ci = mi mod n.

2.5 Algoritma Dekripsi Pesan

Untuk dekripsi pesan, digunakan algoritma sebagai berikut :

1) memakai kunci privat (d,n).
2) Pilih ciphertext dari C
3) Setiap blok ci didekripsikan menjadi blok mi, dengan rumus mi = ci mod n.

2.6 Penggunaan Algoritma RSA

Contoh penggunaan algoritma RSA, sebagai berikut :

Misalkan p=47 dan q= 71 (keduanya prima), kemudian menghitung nilai n = p . q = 47 . 71 = 3337, m = (p - 1)(q - 1) = (47 – 1)(71 -1) = 3220 pilih kunci e = 79, karena 79 relatif prima dengan 3220, maka e dan n bisa di publikasikan ke umum.

Lalu, selanjutnya akan dihitung kunci dekripsi d menggunakan: d = e-1 mod m atau e.d (mod m) = 1 sehingga dapat diperoleh (e=79 dan m=3220): 79. d mod 3220 = 1 dengan mencoba nilai-nilai d = 1,2,3, …, diperoleh nilai kunci pribadi yang bulat dengan 1019. Ini adalah kunci dekripsi yang harus di rahasiakan.

Pesan yang akan dikirim adalah M = TEGUH atau dalam decimal (kode ASCII) adalah: 8469718572, nilai tersebut dipecah menjadi blok-blok m. Maka blok yang akan terbentuk adalah:
M1 = 84; M2 = 69; M3 = 71; M4 = 85; M5 = 72;
sebelumnya telah diketahui kunci publik adalah e = 79 dan n = 3337. Maka pesan M dapat dienkripsikan, yakni:
C1 = 8479 mod 3337 = 1995;
C2 = 6979 mod 3337 = 1689;
C3 = 7179 mod 3337 = 1988;
C4 = 8579 mod 3337 = 3048;
C5 = 7279 mod 3337 = 285;
sehingga ciphertext yang dihasilkan adalah :
1995, 1689, 1988, 3048, 285

Selanjutnya pesan yang telah dienkripsi tersebut dikirim kepada penerima pesan, yang mana telah memiliki kunci pribadi (d,m) = (1019, 3337) sehingga:
M1 = 19951019 mod 3337 = 84;
M2 = 16891019 mod 3337 = 69;
M3 = 19881019 mod 3337 = 71;
M4 = 30481019 mod 3337 = 85;
M5 = 2851019 mod 3337 = 72;
maka akan dihasilkan kembali M = 8469718572, yang dalam pengkodean ASCII dapat dibaca sebagai M = TEGUH.

3. METODOLOGI PENELITIAN

3.1 Studi Literatur

Metode ini menggunakan pembelajaran dengan cara mengumpulkan, membaca dan memahami jurnal, makalah serta refrensi lain untuk mendapatkan informasi yang dibutuhkan dalam mendukung penelitian.

3.2 Analisis Data

Menganalisa Algoritma kriptografi yang digunakan penulis, yaitu Algoritma RSA, serta teknik-teknik yang digunakan.

3.3 Perancangan Sistem

Merancagn sistem aplikasi untuk mengimplementasikan algoritma RSA, serta teknik-tenik yang digunakan.

3.4 Implementasi

Melakukan tahapan untuk mengembangkan perangkat lunak dengan pengkodean program, pengujian, dan menerapkan berdasarkan hasil analisa kedalam bentuk program dengan bahasa pemograman Java.

3.5 Pengujian Sistem

Metode ini dilakukan dengan menguji dan mengawasi jalannya program.

4. ANALISA DAN PERANCANGAN SISTEM

4.1 Analisa Masalah dan Penyelesaiannya

Dizaman yang sudah modern dan perkembangan teknologi semakin pesat sering kali keamanan pada sebuah database disepelekan, dikarenakan keamanan menjadi hal yang kesekian dibandingkan yang lain, namun pada kenyataannya saat ini jika sebuah database diabaikan keamanannya akan menimbulkan kerugian yang besar baik untuk database pribadi, organisasi, lembaga, dan perusahaan. Hal ini terjadi karena database yang disimpan dalam bentuk asli tidak dilakukan pengamanan terlebih dahulu, sehingga pada saat database berhasil dicuri maka database tersebut bisa langsung dibuka dan dibaca oleh orang lain yang tidak berkepentingan atau orang yang tidak berhak atas database tersebut yang mengakibatkan informasi dalam database tersebut tidak terjaga kerahasiaannya sehingga dapat dengan mudah diketahui orang lain..

Untuk menyelesaikan masalah diatas, maka dibuatlah suatu aplikasi yang dapat menjaga kerahasiaan dari sebuah database. Aplikasi tersebut nantinya dapat mengubah sebuah database menjadi database yang isinya tidak bisa dibaca dan database tersebut terjaga kerahasiaannya. Kemudian mengembalikan database tersebut menjadi seperti semula tanpa mengalami perubahan dalam isinya sedikitpun. Dengan adanya aplikasi ini diharapkan suatu database atau database penting dapat disimpan dan dikirim ke pihak yang benar-benar berhak dan tidak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab

4.2 Gambaran Umum Aplikasi

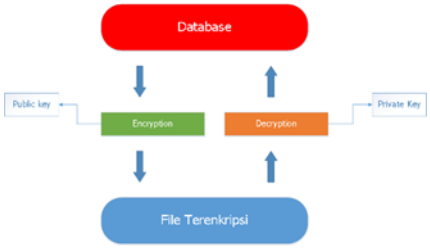
Kebutuhan sistem yang akan dibutuhkan pada aplikasi ini adalah sebagai berikut :

a. Proses pengamanan database dilakukan menggunakan aplikasi berbasis desktop.
b. Aplikasi mampu mengubah database asli menjadi database acak dan juga mampu mengembalikan database acak tersebut menjadi database asli tanpa adanya perubahan pada isi database tersebut.
c. Aplikasi mampu digunakan dengan mudah oleh pengguna yang memahami database.

4.3 Rancangan Aplikasi

Aplikasi terdiri dari beberapa *Form*, yaitu *form Login*, *Main Menu*, *Generate Key*, *Encryption*, *Decryption*, *Guide*, *How To Generate key*, *How To Encryption*, *How To Decryption* dan *Profile*. Untuk dapat melakukan proses enkripsi database maka user bisa menggunakan Menu Encryption dengan memilih basis data yang akan dienkripsi dan menggunakan *Public Key* untuk dapat mengenkripsi database. Selanjutnya akan tampil *output* berupa hasil informasi database yang telah dienkripsi tersebut.

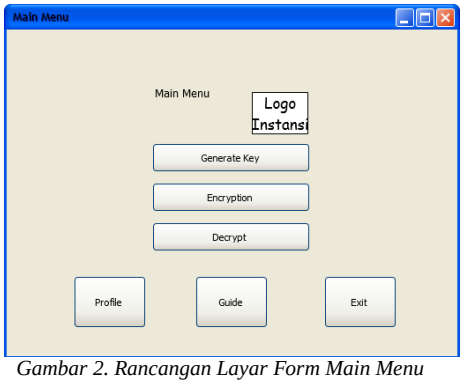
Sedangkan untuk mengembalikan database acak yang sudah dienkripsi menjadi database asli, user dapat memilih menu Decryption, namun user harus memiliki Private Key agar database yang acak tadi dapat kembali menjadi database asli. Serta ada menu help untuk membantu user dalam menggunakan program. User dapat menggunakan Menu Generate Key untuk mendapatkan Public Key dan Private Key yang dibutuhkan. Secara umum, rancangan program yang akan dibuat dapat diilustrasikan pada gambar 1.



Gambar 1. Arsitektur Kerja Aplikasi

4.4 Rancangan Layar Form Main Menu

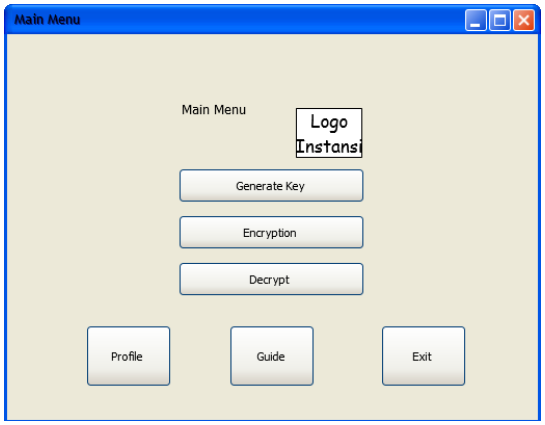
Rancangan Form Main Menu akan keluar setelah pengguna berhasil melewati tahap login. Didalamnya terdapat menu pembuatan kunci (generate key), enkripsi (encryptiion), dekripsi (decryption), profil (profile), bantuan (guide), dan exit untuk keluar dari aplikasi. Selengkapnya bisa dilihat pada gambar 2.



Gambar 2. Rancangan Layar Form Main Menu

4.5 Rancangan Layar Form Generate Key

Dibawah ini adalah gambar dari rancangan layar yang berfungsi untuk pembuatan sepasang kunci, yaitu menu generate key. Bisa dilihat pada gambar 3 dibawah ini.



Gambar 3. Rancangan Layar Generate Key

4.6 Rancangan Layar Form Encryption

Dibawah ini adlaah gambar dari rancangan layar yang berfungsi untuk enkripsi database, yaitu menu encrytion. Bisa dilihat pada gambar 4 dibawah ini.

Gambar 4. Rancangan Layar Encryption

4.7 Rancangan Layar Form Decryption

Dibawah ini adalah gambar dari rancangan layar yang berfungsi untuk pengembalian database yang sudah dienkrip. Yaitu menu decryption. Bisa dilihat pada gambar 5 dibawah ini.

Gambar 5. Rancangan Layar Decryption

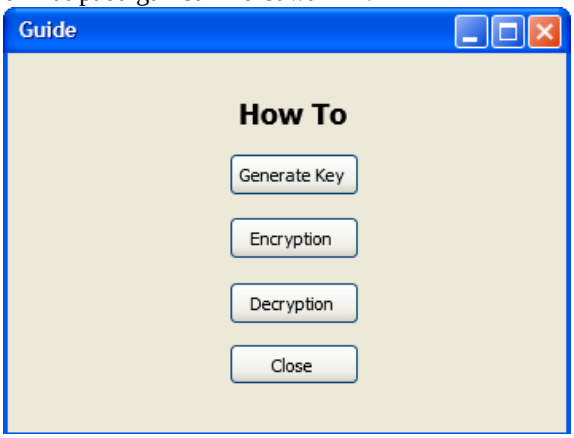
4.8 Rancangan Layar Form Profile

Dibawah ini adlaah gambar dari rancangan layar profile, digunakan untuk mengetahui profil dari penulis. Bisa dilihat pada gambar 6 dibawah ini.

Gambar 6. Rancangan Layar Profile

4.9 Rancangan Layar Guide

Dibawah ini adalah gambar dari rancangan layar yang berfungsi untuk mengetahui bagaimana cara menggunakan aplikasi ini, yaitu form guide. Bisa dilihat pada gambar 7 dibawah ini.



Gambar 7. Rancangan Layar Guide

5. HASIL DAN PEMBAHASAN

Aplikasi Kriptografi Database tentu harus diujiuntuk dapat mengetahui hasil yang didapatkan setelah sistem dijalankan, fungsi utama aplikasi ini adalah melakukan enkripsi dan dekripsi table database.

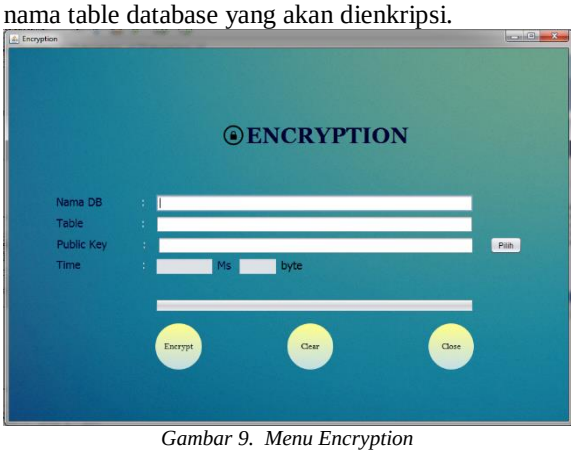
5.1 Tampilan Layar Menu Generate Key

Form Menu Generate Key adalah form yang berfungsi untuk membuat public key dan private key. Key ini nantinya akan digunakan pada saat melakukan proses enkrip dan dekrip database.

Gambar 8. Menu Generate Key

5.2 Tampilan Layar Menu Encryption

Form Menu Encryption adalah form yang berfungsi untuk melakukan enkripsi database. User harus memasukan nama database dan memasukan nama table database yang akan dienkripsi.



Gambar 9. Menu Encryption

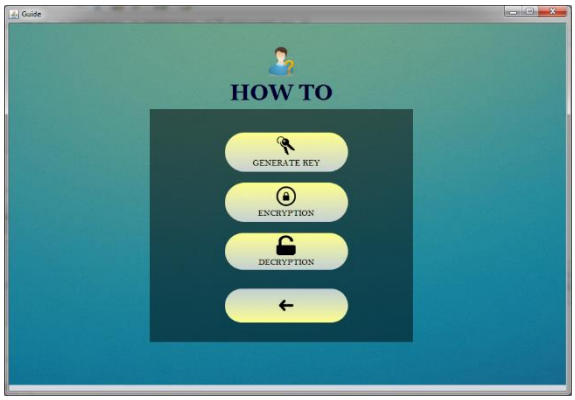
5.3 Tampilan Layar Menu Decryption

Form Menu Decryption adalah form yang berfungsi untuk melakukan dekripsi database. User harus memasukan nama database dan memasukan nama table database yang telah dienkripsi sebelumnya.

Gambar 10. Tampilan Menu Decryption

5.4 Tampilan Layar Menu Guide

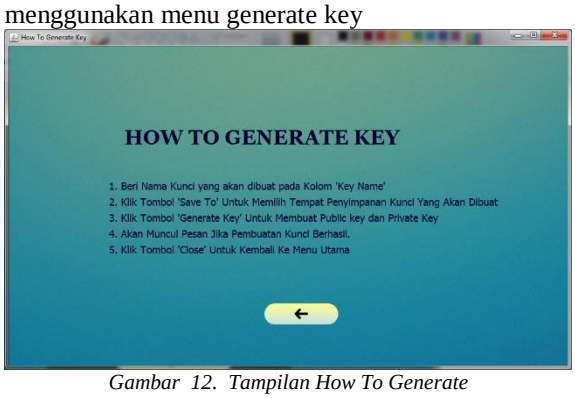
Form Menu Guide adalah form yang berfungsi untuk mengetahui bagaimana cara menggunakan aplikasi ini.



Gambar 11. Tampilan Menu Guide

5.5 Tampilan Layar How To Generate Key

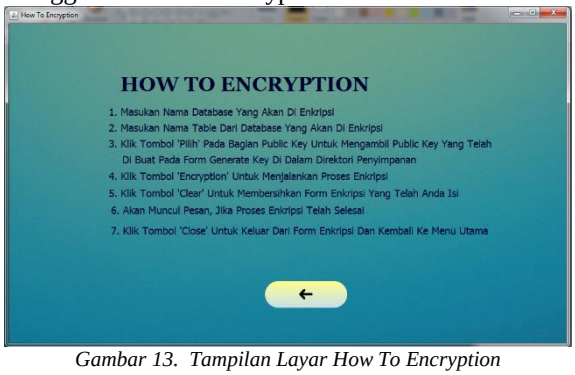
Form Menu How To Generate Key adalah form yang berfungsi untuk mengetahui bagaimana cara menggunakan menu generate key



Gambar 12. Tampilan How To Generate

5.6 Tampilan Layar How To Encryption

Form How To Encrypion adalah form yang berfungsi untuk mengetahui bagaimana cara menggunakan form encryption



Gambar 13. Tampilan Layar How To Encryption

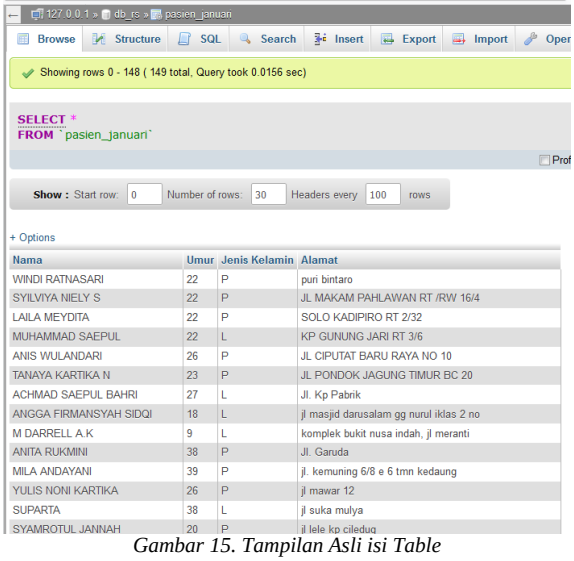
5.7 Tampilan Layar How To Decryption

Form How To Decryption adalah form yang berfungsi untuk mengetahui bagaimana cara menggunakan form decryption

Gambar 14. Tampilan Layar How To Decryption

5.8 Pengujian Program

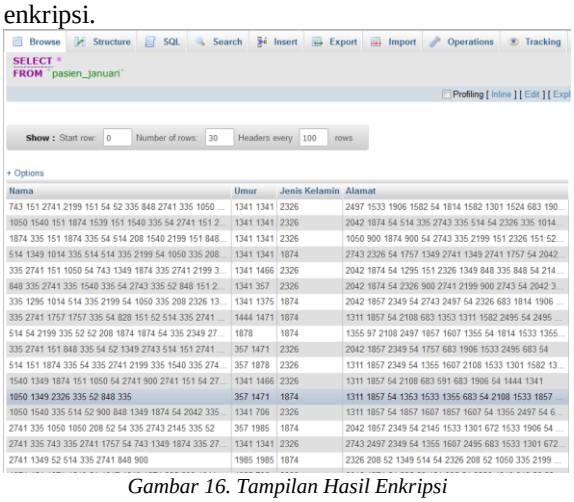
Berikut adalah proses dari pengamanan isi dari tabel database)



Nama	Umur	Jenis Kelamin	Alamat
WINDI RATNASARI	22	P	puri bintaro
SYILVIYA NIELY S	22	P	JL MAKAM PAHLAWAN RT /RW 16/4
LAILA MEYDITA	22	P	SOLO KADIPIRO RT 2/32
MUHAMMAD SAEPUL	22	L	KP GUNUNG JARI RT 3/6
ANIS WULANDARI	26	P	JL CIPUTAT BARU RAYA NO 10
TANAYA KARTIKA N	23	P	JL PONDOK JAGUNG TIMUR BC 20
ACHMAD SAEPUL BAHRI	27	L	Jl. Kp Pabrik
ANGGA FIRMANSYAH SIDQI	18	L	jl masjid darusalam gg nurul iklas 2 no
M DARRELL A.K	9	L	komplek bukit nusa indah, jl meranti
ANITA RUKMINI	38	P	Jl. Garuda
MILA ANDAYANI	39	P	jl. kemuning 6/8 e 6 tmn kedaung
YULIS NONI KARTIKA	26	P	jl mawar 12
SUPARTA	38	L	jl suka mulya
SYAMROTUL JANNAH	20	P	jl lele kp cileduq

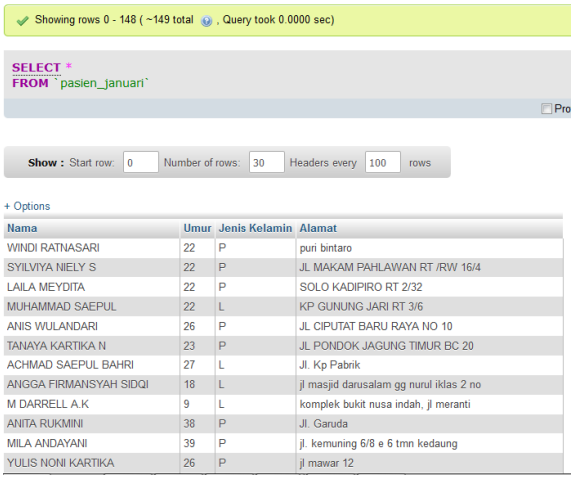
Gambar 15. Tampilan Asli isi Table

Berikut ini merupakan tampilan database dengan isi acak yang berhasil melalui proses enkripsi.



Gambar 16. Tampilan Hasil Enkripsi

Selanjutnya adalah gambar dari isi database yang sudah didekripi.



Nama	Umur	Jenis Kelamin	Alamat
WINDI RATNASARI	22	P	puri bintaro
SYILVIYA NIELY S	22	P	JL MAKAM PAHLAWAN RT /RW 16/4
LAILA MEYDITA	22	P	SOLO KADIPIRO RT 2/32
MUHAMMAD SAEPUL	22	L	KP GUNUNG JARI RT 3/6
ANIS WULANDARI	26	P	JL CIPUTAT BARU RAYA NO 10
TANAYA KARTIKA N	23	P	JL PONDOK JAGUNG TIMUR BC 20
ACHMAD SAEPUL BAHRI	27	L	Jl. Kp Pabrik
ANGGA FIRMANSYAH SIDQI	18	L	jl masjid darusalam gg nurul iklas 2 no
M DARRELL A.K	9	L	komplek bukit nusa indah, jl meranti
ANITA RUKMINI	38	P	Jl. Garuda
MILA ANDAYANI	39	P	jl. kemuning 6/8 e 6 tmn kedaung
YULIS NONI KARTIKA	26	P	jl mawar 12

Gambar 17. Tampilan Hasil Dekripsi

6. KESIMPULAN

Setelah melewati tahap pembuatan dan pengujian program ini, dapat disimpulkan bahwa :

1. Proses enkripsi dan dekripsi pada database berhasil dilakukan. Database asli dapat dienkripsi menjadi database yang disandikan dan dapat didekripsi menjadi database asli kembali.
2. Keamanan database pada menjadi lebih kuat karena aplikasi ini menggunakan Algoritma RSA.
3. Proses enkripsi dan dekripsi tergolong cepat, meskipun jumlah Record di dalam Table cukup banyak.

7. DAFTAR PUSTAKA

[1] Kromodimoeljo, S. 2010. Teori dan Aplikasi Kriptografi. Jakarta: SPK IT Consulting.

[2] Antonius Wahyu Sudrajat. 2016. Implementasi Enkripsi Database Menggunakan Transparent Data Encryption pada Database Engine Oracle. Jurnal Imiah STMIK GI MDP, Vol 2 No 3.

[3] Akbar Bahroni. 2015. Pengamanan Record Database Menggunakan Kriptografi Algoritma RSA.

[4] Saipul Bahri, Diana, dan Susan Dian PS. 2012. Studi dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5.

[5] Pahrizal dan David Pratama. 2016. Implementasi Algoritma RSA Untuk Pengamanan Data Berbentuk Teks.

[6] Prasetyo Andy Wicaksono. 2014. Enkripsi Menggunakan Algoritma RSA.

[7] Abdul Kadir. 2002, Konsep & Tuntutan Praktis Basis Data, Yogyakarta: Penerbit Andi.