PENGEMBANGAN APLIKASI ENKRIPSI DAN DEKRIPSI RECORD-RECORD DATABASE PADA DBMS MYSQL MENGGUNAKAN ALGORITMA AFFINE CIPHER BERBASIS JAVA

Humuntal Rumapea, Ely Sawato Zebua
Sistem Informasi, Fakultas Ilmu Komputer, Universitas Methodist Indonesia

hrumapea1608@gmail.com, Elyzebua@gmail.com

ABSTRAK

Database saat ini sudah sangat dikenal sebagai media penyimpanan data- data, baik yang bersifat publik maupun data-data yang bersifat personal. Banyaknya pengguna database, membuat data yang ada di dalam database itu sendiri dapat dengan mudah diakses oleh pengguna-pengguna yang tidak memiliki hak akses untuk itu. Demi menciptakan keamanan untuk data-data yang bersifat personal, DBMS menciptakan sebuah sistem keamanan tersendiri. Penelitian ini bertujuan untuk membangun sebuah aplikasi yang dapat menggantikan sistem keamanan dari DBMS itu sendiri terkhusus DBMS Mysql dengan menggunakan algoritma kriptografi Affine Cipher yang mudah dan cepat. Metodologi penelitian yang dilakukan meliputi studi pustaka serta pengembangan sistem menggunakan metode Rapid Application Development (RAD). Studi pustaka dilakukan dengan cara mengumpulkan data-data dari uraian-uraian teoritis, dan untuk mengimplementasikan rancangan digunakan pemrograman Java. Hasil dari penelitian ini merupakan Aplikasi Enkripsi dan Dekripsi record- record DBMS Mysql yang dapat memudahkan pengguna dalam mengamankan informasi-informasi yang ada di dalam database Mysql dari pihak yang tidak diinginkan serta dapat mengembalikan database Mysql kembali ke dalam bentuk aslinya.

Keyword : *Keamanan Database, Affine Cipher, Mysql, Java).*

I. PENDAHULUAN

Database saat ini sudah sangat dikenal sebagai media penyimpanan data-data, baik yang bersifat publik maupun data-data yang bersifat personal. Publik diartikan sebagai data yang isi dan seluruh kapasitasnya dapat diketahui oleh seluruh khayalak. Berbeda dengan publik, personal lebih dikhususkan untuk data-data yang hanya dapat diketahui dan dimanipulasi oleh beberapa pihak yang dikhususkan untuk itu. Dilihat dari itu, dapat disimpulkan bahwa data yang bersifat personal tentu memiliki tingkat kerahasiaan yang tinggi.

Demi menciptakan keamanan untuk data-data yang bersifat personal, DBMS menciptakan sebuah sistem keamanan tersendiri. Sistem keamanan tersebut umumnya dikenal sebagai Data Security Language (DSL) sebuah bahasa khusus yang diciptakan untuk itu. Selain itu, ada juga DBMS yang membuat sistem tingkatan user, dimana setiap user memiliki akses- akses yang berbeda satu dengan yang lain. Namun, seiring dengan berjalannya waktu, sistem keamanan yang seperti disebutkan diatas sudah ditemukan banyak celah oleh pihak- pihak yang ingin menembusnya.

Mysql merupakan salah satu DBMS yang banyak digunakan karena sifat open source yang dimilikinya. Banyaknya pengguna Mysql membuat Mysql semakin giat menguatkan sistem keamanannya. Beberapa tahun terakhir, Mysql menerapkan konsep kriptografi modern yang terintegrasi ke dalam sistemnya. Namun banyaknya pengguna Mysql menyebabkan adanya celah untuk menembus sistem tersebut. Adanya aplikasi yang dapat menggantikan fungsi kriptografi yang terintegrasi dalam

DBMS Mysql dirasa dapat meminimalkan ancaman yang datang dari pihak yang ingin menembus sistem keamanan DBMS Mysql. Aplikasi tersebut diharapkan dapat meningkatkan keamanan data-data yang tersimpan dalam database di DBMS Mysql serta diharapkan dapat lebih mudah dan cepat. Salah satu algoritma kriptografi yang bersifat mudah dan cepat adalah metode Affine Cipher. Berdasarkan uraian tersebut diatas, penulis mencoba melakukan penelitian dengan mengambil judul **"**Perancangan Aplikasi Enkripsi dan Dekripsi Record-record Database pada DBMS Mysql menggunakan algoritma Affine Cipher berbasis Java" .

2. TINJAUAN PUSTAKA

Keamanan Komputer

Menurut Kamus Besar Bahasa Indonesia, kata "aman" berarti bebas dari bahaya, bebas dari gangguan, terlindung atau tersembunyi, tentram dan tidak mengandung resiko. Sehingga dapat diartikan, arti kata keamanan mengacu pada hal atau keadaan yang bebas dari bahaya ataupun gangguan.

Dari pengertian diatas dapat disimpulkan bahwa, keamanan komputer merupakan sebuah aspek yang menandakan sebuah sistem komputer yang terlindung serta bebas dari bahaya dan gangguan.

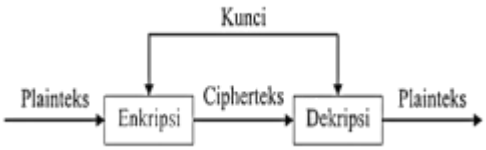
Basis Data

Menurut Fathansyah (2015:12), Sistem basis data merupakan sistem yang terdiri atas kumpulan tabel data yang saling berhubungan (dalam sebuah basis data di sebuah sistem komputer) dan sekumpulan program (yang biasa disebut DBMS/*Data Base Management System*) yang memungkinkan beberapa pemakai dan/atau program lain untuk mengakses dan memanipulasi tabel- tabel data tersebut.

Kriptografi

Kriptografi berasal dari bahasa Yunani. Terdiri dari 2 kata yaitu "*kryptós*" yang berarti tersembunyi dan "*gráphein"* yang berarti tulisan. Dengan arti kata tersebut dapat disimpulkan bahwa kriptografi adalah tulisan yang tersembunyi.

Menurut Munir (2006), kriptografi dapat digambarkan dengan skema dibawah ini :



Gambar 1 Skema Kriptografi
Sumber : Kriptografi (Munir : 2006)

Metode Affine Cipher

Menurut Munir (2006:35), Metode Affine Cipher merupakan salah satu metode kriptografi klasik yang merupakan perluasan dari metode Caesar Cipher yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. Secara matematis enkripsi plainteks P lalu menghasilkan C dapat dinyatakan dengan persamaan seperti di bawah ini :

$Ci = mPi + K(\text{mod } n)$ (2.1)

dengan persamaan dekripsi sebagai berikut :

$P = m^{-1} (C-K)(\text{mod } n)$ **(2.2)**

dimana :
Ci = karakter cipherteks yang akan dicari,
m = bilangan bulat yang relatif prima dengan n,
m^{-1}= invers m,
Pi = karakter plainteks, K = kunci,
n = ukuran alfabet.

Mysql

Mysql adalah sebuah sistem manajemen database relasi (relational database management system) yang bersifat open source. MySQL merupakan buah pikiran dari Michael "Monty" Widenius, David Axmark dan Allan Larson yang di mulai tahun 1995. mereka bertiga kemudian mendirikan perusahaan bernama MySQL AB di Swedia.

Unified Modelling Language

Unified Modelling Language merupakan salah satu alat bantu yang dapat digunakan dalam bahasa pemrograman yang berorientasi objek.(informatika.web.id/pengertian -uml, diakses tanggal 1 Maret 2017). Menurut Rosa, Salahuddin (2016:137), UML muncul karena adanya kebutuhan pemodelan visual untuk menspesifikasikan, menggambarkan, membangun, dan dokumentasi dari sistem perangkat lunak.

3. METODOLOGI PENELITIAN

Penelitian yang akan dilakukan menggunakan tahapan sebagai berikut :

1. Studi Kepustakaan

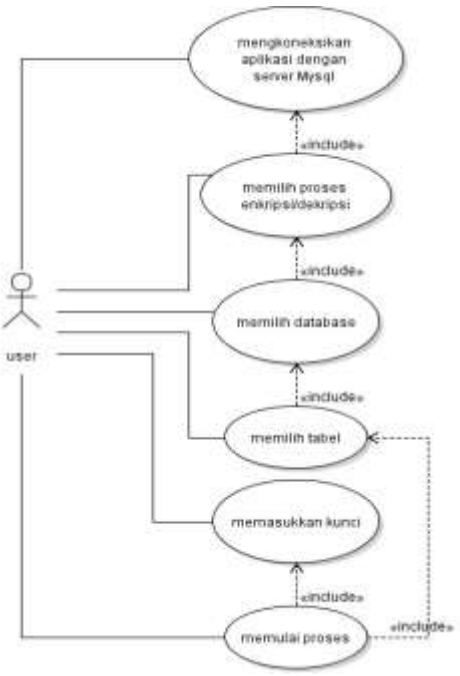
Merupakan pencarian literature-literature yang dapat mendukung penyelesaian sistem aplikasi ini, terutama algoritma Kriptografi dan Bahasa Pemrograman yang dipergunakan. Literature yang dimaksud dapat berupa buku-buku, paket modul dan panduan dan segala kepustakaan lainnya yang dianggap perlu dan mendukung.

2. Pengembangan Aplikasi
Metode Pengembangan Aplikasi yang digunakan dalam penelitian ini adalah metode Rapid Application Development(RAD)

3. Penulisan Laporan
Merupakan tahapan penulisan laporan dari hasil penelitian yang dilakukan dan hasil ujicoba penelitian.

4. HASIL DAN PEMBAHASAN

A. Hasil
Desain atau perancangan dalam pembangunan perangkat lunak merupakan upaya untuk mengontruksi sebuah sistem yang memberikan kepuasan (mungkin informal) akan spesifikasi kebutuhan fungsional, memenuhi target, memenuhi kebutuhan secara implisit atau eksplisit dari segi performansi maupun dari segi biaya, waktu dan perangkat. (Rosa A.S, M. Shalahuddin:2016)

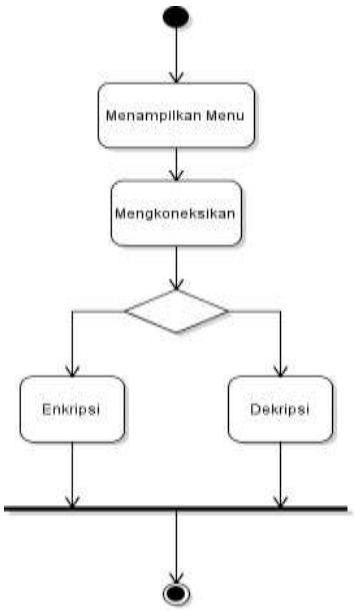


Gambar 2. Use Case Diagram

A. Pembahasan
Adapun analisa langkah- langkah yang diperlukan untuk mengenkripsi record-record database Mysql adalah sebagai berikut :

1. Aplikasi menyimpan nama database yang akan dienkripsi dalam sebuah variabel dan menyimpan nama-nama tabel ke dalam variabel array.
2. Nama database dienkripsi menggunakan fungsi enkripsi affine cipher kemudian dibuat database baru dengan nama database yang telah dienkripsi.

3. Masing-masing field dari tiap-tiap tabel diambil kemudian disimpan ke dalam array 2 dimensi. Hal yang sama dilakukan juga untuk tipe data tiap field.
4. Semua nama tabel serta seluruh field-fieldnya dienkripsi.
5. Dengan menggunakan perulangan, tabel baru dibuat pada database yang telah dibuat sebelumnya. dengan nama tabel serta nama field yang telah dienkripsi.
6. Kunci serta bilangan relatif prima dienkripsi lalu dimasukkan kedalam sebuah tabel sebagai informasi untuk proses pendekripsian.
7. Satu per satu record diambil dan dienkripsi serta langsung ditambahkan ke dalam tabel yang telah dienkripsikan sebelumnya.
8. Proses enkripsi akan berakhir jika semua record telah terenkripsi.



Gambar 3. Diagram Aktivity

Adapun tampilan aplikasi yang dirancang seperti berikut ini:

1. Tampilan Utama

Tampilan utama menampilkan menu-menu utama Aplikasi Enkripsi Dekripsi record-record Database DBMS Mysql seperti gambar di bawah ini :

Gambar 4. Tampilan utama.

2. Tampilan Form Dekripsi

Form dekripsi berfungsi untuk mengembalikan database yang telah dienkripsi ke dalam bentuk aslinya.

Gambar 5. Tampilan Form Dekripsi

5. KESIMPULAN

Berdasarkan uraian dan penjelasan serta pembahasan keseluruhan materi, maka diambil kesimpulan sebagai berikut :

1. Dengan adanya aplikasi yang telah dibangun, pengguna Mysql dapat mengubah data pada record-record databasenya menjadi tidak dapat diketahui
2. Aplikasi yang telah dibangun juga dapat menerjemahkan kembali data-data yang telah diubah menjadi bentuk aslinya
3. Proses enkripsi serta dekripsi pada aplikasi yang telah dibangun mengubah per database bukan per record.

6. REFERENSI

[1]. Agung, H., Budiman. 2015. Implementasi Affine Chiper Dan Rc4 Pada Enkripsi File Tunggal., ISBN:978-602-1180-21-1., VOL.1.
[2] A.S. Rosa., Shalahuddin. M. 2016. Rekayasa Perangkat Lunak. Informatika. Bandung.
[3] Bambang Hariyanto. 2005. Esensi- esensi Bahasa Pemrograman Java, Informatika, Bandung.
[4] Elmasri, Ramez. 2010. Fundamental of Database Systems (6th Edition).
[5] Fathansyah. 2015. Basis Data. Informatika. Bandung.
[6] Kadir, Abdul. 2007. Dasar Pemrograman Java. Andi. Yogyakarta.
[7] Kromodimoeljo, Sentot. 2009. Teori Dan Aplikasi Kriptografi. SPK IT Consulting.
[8] Menezes, Alfred J., Paul C van Oorschot, dan Scott A. Vanstone. 1996. Handbook of Applied Cryptography. CRC Press.
[9] Munir,R. 2006. Kriptografi. Informatika. Bandung.
[10] Setyaningsih, Emy. 2015. Kriptografi & Implementasinya menggunakan MATLAB. Andi. Yogyakarta.