

BAB I

PENDAHULUAN

I.1. Latar Belakang

Basis data (*database*) sangat banyak digunakan untuk menyimpan data dan informasi yang penting. Basis data (*database*) adalah tempat untuk menyimpan data dan nantinya data ini bisa diambil lagi. Tanpa *database aplikasi* akan kesulitan menyimpan data. Banyak terdapat jenis-jenis yang dapat digunakan oleh pengguna komputer diantaranya yaitu *MS. Access, SQL Server 2008, MySQL, Postgres MySQL* dan lain sebagainya. Namun kebanyakan orang menggunakan *MySQL* untuk penyimpanan data karena selain penggunaannya yang mudah dan gratis untuk digunakan, *MySQL* dapat menampung jumlah data yang sangat banyak. Data yang tersimpan pada *MySQL* umumnya tersimpan pada *localhost* dan data dalam *MySQL* juga dapat disimpan dalam bentuk *script*, sehingga pengguna dapat dengan mudah memindahkan data *MySQL* ke komputer lain. Namun akan menjadi masalah ketika orang yang berniat jahat mendapatkan *script* tersebut. Isi data yang berharga di dalam basis data *MySQL* dapat dicuri dan digunakan oleh pihak yang tidak diinginkan, sehingga merugikan pemilik isi basis data *MySQL*.

Oleh karena itu dibutuhkan sebuah cara yang dapat diterapkan untuk keamanan pada isi sebuah basis data *MySQL*. Cara yang dapat digunakan yaitu menerapkan kriptografi pada isi sebuah basis data *MySQL*. Kriptografi adalah seni tentang bagaimana agar teks menjadi aman dengan cara mengubah teks tersebut

menjadi bentuk yang tidak dapat dibaca. Teks yang asli dan masih dapat terbaca disebut sebagai *plain text*, sedangkan teks yang tidak dapat dibaca dan tidak bermakna disebut sebagai *cipher text*. Proses pengubahan *plain text* menjadi *cipher text* disebut sebagai enkripsi (*encryption*), sedangkan proses pengembaliannya disebut sebagai dekripsi (*decryption*). Dalam penggunaan kriptografi diperlukan adanya metode yang dapat memproses sebuah pesan asli menjadi pesan rahasia. Oleh karena itu peneliti merekomendasikan metode *rail fence cipher*. *Rail Fence Cipher* merupakan salah satu variasi implementasi *cipher* transposisi. Pada *Rail Fence Cipher*, plainteks dituliskan secara vertikal ke bawah sepanjang *n-rails*, dan menulis lagi ke kolom baru ketika telah mencapai karakter ke-*n*. *Cipher text* yang dihasilkan adalah urutan karakter yang dibaca secara horizontal. Namun metode *rail fence cipher* hanya bersifat mengacak karakter dan tidak memiliki perubahan karakter seperti halnya pada metode kriptografi yang lain, sehingga keamanannya masih dapat diragukan. Oleh karena itu peneliti menambahkan metode ROT13 pada metode *rail fence cipher*. ROT13 (*Rotate 13*) adalah enkripsi *substitution cipher* yang umum digunakan di sistem operasi *UNIX*. Pada sistem enkripsi ROT13 sebuah huruf digantikan dengan huruf yang letaknya di atas 13 posisi darinya. Sehingga dengan adanya penambahan 13 abjad maka metode *rail fence cipher* akan menghasilkan keamanan yang lebih baik.

Dengan latar belakang diatas maka peneliti mengangkat judul **“Penerapan Metode Rail Fence Cipher Dan ROT13 Untuk Keamanan Script MySQL”**.

I.2. Ruang lingkup Permasalahan

Ruang lingkup permasalahan yang dapat dijabarkan berdasarkan latar belakang adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Dari latar belakang pemilihan judul, maka identifikasi masalah dari peneliti untuk skripsi ini adalah sebagai berikut :

1. *Script MySQL* tidak memiliki keamanan.
2. Dibutuhkan metode kriptografi yang tepat untuk keamanan *script MySQL*.

I.2.2. Perumusan Masalah

Perumusan masalah yang berdasarkan identifikasi masalah yang terdapat pada penelitian ini adalah sebagai berikut :

1. Bagaimana memberikan keamanan pada *script MySQL* ?
2. Bagaimana menerapkan metode *Rail Fence Cipher* dan metode ROT13 untuk keamanan *script MySQL* ?

I.2.3. Batasan Masalah

Disebabkan banyaknya permasalahan dan waktu yang terbatas, maka agar pembahasan masalah tidak melebar penulis membatasi masalah sebagai berikut :

1. Aplikasi hanya untuk mengamankan *script MySQL*.
2. Aplikasi hanya dapat berjalan pada sistem operasi *windows*.
3. *Input* aplikasi ini berupa teks asli *script*.
4. *Output* aplikasi ini berupa teks *script* yang tersandi.
5. Pembuatan aplikasi ini menggunakan pemrograman *Visual basic 2010*.

6. Perancangan aplikasi ini menggunakan pemodelan *Unified Modelling Language* (UML).
7. Metode yang digunakan adalah metode *Rail Fence Cipher* dan ROT13.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Menghasilkan aplikasi keamanan *Script MySQL* menggunakan metode *Rail Fence Cipher* dan metode ROT13.
2. Memberikan keamanan data pada script MySQL.

I.3.2. Manfaat Penelitian

Manfaat yang dihasilkan penelitian ini adalah sebagai berikut :

1. Mengetahui penggunaan metode *Rail Fence Cipher* dan metode ROT13 untuk keamanan *Script MySQL*.
2. *Script MySQL* mendapatkan penambahan keamanan data.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematis untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan. Tahapan dalam penelitian ini dapat di modelkan pada diagram *Fish Bone*. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :

I.4.1. Pengumpulan Data

Dalam pengumpulan data-data yang diperlukan dalam penyusunan penelitian ini, maka peneliti menggunakan beberapa tahapan yaitu :

1. Sampel (*Sampling*)

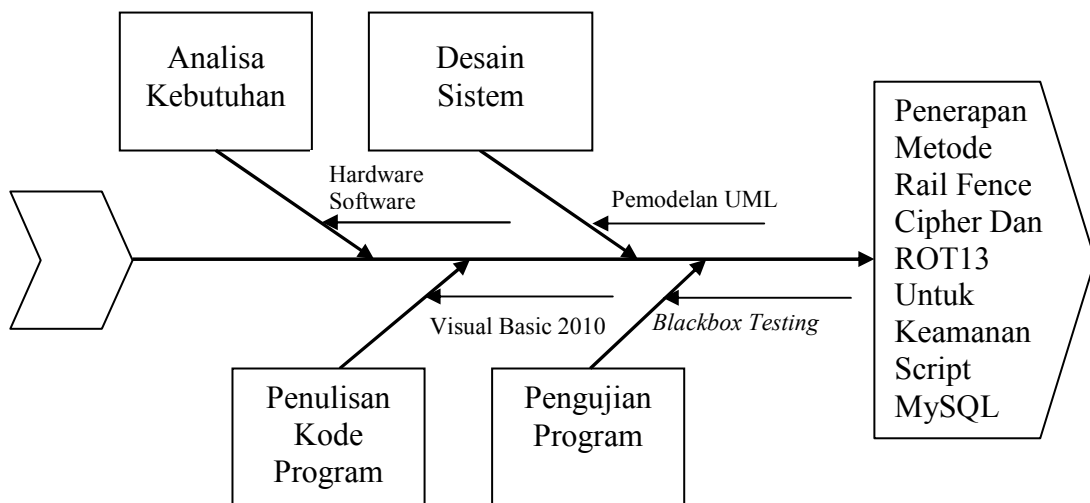
Peneliti mengumpulkan contoh-contoh penelitian terdahulu berupa referensi dan aplikasi.

2. Penelitian perpustakaan (*Library Research*)

Pada metode ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi yang dikutip dapat berupa teori yaitu jurnal mengenai keamanan, metode *railfence cipher* dan metode ROT13.

1.4.2. *Fish Bone* Metode Penelitian

Berikut adalah *fish bone* metode penelitian yang digunakan dalam penulisan skripsi ini.



Gambar I.1. Diagram *Fish Bone* Metodologi Penelitian

Keterangan :

1. Analisis Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan yaitu *hardware* dan *software* yang akan digunakan untuk menyelesaikan penelitian.

2. Desain Sistem

Desain sistem yang digunakan dalam teori adalah pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Penulisan kode program menggunakan bahasa pemrograman *visual basic* 2010 dan menggunakan *database* MySQL.

4. Pengujian Program

Pengujian program merupakan langkah yang dilakukan setelah penulisan kode program. Pengujian program secara teori peneliti menggunakan teknik pengujian *blackbox testing* yang disajikan dalam bentuk tabel. Pengujian program secara praktek peneliti menggunakan *visual basic* 2010.

5. Hasil

Pada tahapan hasil penelitian telah selesai dilakukan dan menghasilkan aplikasi penerapan metode *Rail Fence Cipher* dan ROT13 untuk keamanan *script MySQL*.

1.5. Kontribusi Penelitian

Kontribusi yang dihasilkan penelitian ini adalah sebagai berikut :

1. Penelitian ini dapat menjadi referensi baru bagi peneliti berikutnya.
2. Penelitian ini dapat memberikan pengembangan ide bagi peneliti berikutnya.

3. Penelitian ini dapat memberikan keamanan pada *script* basis data MySQL.

I.6. Sistematika Penulisan

Sistematika penulisan yang diajukan dalam skripsi ini ialah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan Skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan serta perangkat yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisikan berbagai kesimpulan yang dapat dibuat berdasarkan uraian yang telah disimpulkan dan saran.