BAB I

PENDAHULUAN

I.1. Latar Belakang

Pentingnya sebuah informasi dalam kehidupan membuat orang-orang berlomba-lomba dan hantusias untuk mendapatkan informasi lebih dahulu dari orang lain, karena dengan adanya informasi yang penting mereka dapat mengolah data sehingga menjadi informasi yang baru. Dengan adanya informasi yang baru orang-orang dapat menghasilkan uang yang banyak. Pada zaman sekarang ini penggunaan teknologi komputer sudah berkembang menjadi sangat pesat, sehingga informasi banyak disimpan dan diolah melalui teknologi komputer. Penggunaan komputer untuk mengelola informasi sudah dipakai di kalangan dunia bisnis, pelajar dan lain sebagainya. Informasi yang telah diolah biasanya menjadi sebuah data yang sangat rahasia, kebanyakan orang menyimpan data-data pribadi mereka dan merahasiakan dari umum ke dalam sebuah komputer yang biasa disebut *database*. Di dunia bisnis kebanyakan di perusahaannya menggunakan *database MySQL* sebagai aplikasi untuk menyimpan data-data perusahaan, karena *database MySQL* mampu menampung data dalam jumlah yang besar dan kegunaannya yang mudah. Untuk itu menjaga keamanan data menjadi sangat penting bagi mereka. Banyaknya pencuri informasi dan perusak data membuat kalangan pembisnis merasa risau, karena dengan jatuhnya informasi ketangan mereka, bisnis mereka akan berjalan menjadi tidak baik

karena informasi tersebut dapat diolah ataupun dirusak oleh para pencuri data tersebut. (Anisa, 2013).

Perlu adanya keamanan data di dalam komputer terutama *database* agar rahasia informasi mereka tetap terjaga. Untuk itu penulis merekomendasikan sebuah sistem pengamanan data pada *database MySQL*. Pada sistem ini isi data di dalam *database* dapat disandikan, sehingga tidak dapat terbaca oleh pencuri informasi. Namun di dalam penerapannya dibutuhkannya metode untuk menyelesaikan masalah di dalam keamanan data. Untuk itu penulis merekomendasikan dua metode yaitu metode *vernam cipher* dan metode *gronsfeld cipher* agar keamanan datanya lebih terjaga. Metode *vernam cipher* atau biasa dikenal dengan sebutan *one time pad* (*OTP*) merupakan algoritma berjenis *symmetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream cipher* yang berasal dari hasil *XOR* antara bit *plaintext* dan *bit key*. Pada metode ini *plain text* diubah kedalam kode *ASCII* dan kemudian dikenakan operasi *XOR* terhadap kunci yang sudah diubah ke dalam kode *ASCII.* (M. Sholeh dan J.V. Hamokwarong, 2011). Metode *Gronsfeld* adalah satu *cipher* subsitusi sederhana *polyalphabetic.* Gaspar Schot adalah seorang kriptografer abad ke 17 di Jerman, yang belajar *cipher* ini selama perjalanan antara Mainz dan Frankfurt dengan menghitung *Gronsfeld*, maka terciptalah nama dari *chipper* tersebut yaitu *gronsfeld*. *System gronsfeld* menggunakan suatu kunci numeric yang biasanya cukup pendek misalnya 7341, kunci ini diulang secara periodic, sesuai dengan jumlah kata *plaintext.* (Aznuddin, 2013). Dengan latar belakang diatas maka penulis mengambil judul **"Pembelajaran Penyandian Data Di Dalam Database MySQL Menggunakan Metode Vernam Cipher Dan Gronsfeld Cipher".**

I.2. Ruang lingkup Permasalahan

Adapun beberapa tahap yang dilakukan dalam membuat ruang lingkup permasalahan adalah :

I.2.1. Identifikasi Masalah

Dengan mengetahui latar belakang pemilihan judul di atas, maka indentifikasi masalah dari penulis untuk skripsi ini adalah:

1. Diperlukan sebuah keamanan isi *database MySQL*.
2. Diperlukan sebuah metode untuk penyandian *database MySQL*.
3. Diperlukan sebuah perangkat lunak untuk menyandikan data di dalam *database MySQL*.

I.2.2. Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian ini yaitu:

1. Bagaimana tampilan antarmuka aplikasi penyandian data di dalam *database MySQL* menggunakan metode *vernam cipher* dan *gronsfeld cipher*?
2. Bagaimana metode *vernam cipher* dan *gronsfeld cipher* dapat menyandikan isi *database MySQL*?
3. Bagaimana menerapkan aplikasi penyandian data di dalam *database MySQL* menggunakan metode *vernam cipher* dan *gronsfeld cipher* di komputer?

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 menyandikan isi *database MySQL*.
2. Aplikasi tidak dapat menyandikan isi *database* yang bertipe data angka.
3. *Input* aplikasi ini berupa teks untuk disandikan.

4. *Output* aplikasi ini berupa teks yang tersandikan.

5. Perancangan dan pembuatan Aplikasi ini menggunakan bahasa *Microsoft Visual Basic* 2010.

I.3. Tujuan Dan Manfaat

1.3.1 Tujuan

1. Untuk menghasilkan sebuah perangkat lunak yang dapat menyandikan isi *database MySQL*.
2. Untuk mengetahui dan memahami cara kerja dari Metode *Vernam Cipher* dan *Gronsfeld Cipher* di dalam penyandian isi *database MySQL.*.
3. Untuk membantu *user* dalam menyandikan isi *database MySQL*.

1.3.2 Manfaat

1. Mengatasi masalah penyandian isi *database MySQL*.
2. Penulis dapat lebih memahami penggunaan metode *vernam cipher* dan *gronsfeld cipher*.
3. Penulis mendapat wawasan dalam pembuatan aplikasi komputer.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Untuk itu penulis menggunakan beberapa cara untuk memperolehnya, diantaranya :

1. Pengumpulan Data

   Pada tahap ini dilakukan dengan mempelajari teori dasar yang mendukung penelitian, pencarian dan pengumpulan data-data yang dibutuhkan. Untuk mengumpulkan data yang dibutuhkan, maka penulis memakai teknik :

   a. Pengamatan Langsung (*Observation*)

Melakukan pengamatan secara langsung ke tempat objek pembahasan yang ingin diperoleh yaitu bagian-bagian terpenting dalam pengambilan data yang diperlukan berkaitan tentang *database MySQL*.

b. Wawancara (*Interview*)

Teknik ini secara langsung bertatap muka dengan pihak bersangkutan untuk mendapatkan penjelasan dari masalah-masalah yang sebelumnya kurang jelas yaitu tentang mekanisme sistem yang digunakan pada perusahaan dan juga untuk meyakinkan bahwa data yang diperoleh dikumpulkan benar-benar akurat.

c. *Sampling*

Meneliti dan memilih data - data yang tersedia dan sesuai dengan bidang yang dipilih sebagai berkas lampiran.

2. Penelitian perpustakaan (*Library Research*)

Pada metode ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi yang dikutip dapat berupa teori ataupun beberapa pendapat dari beberapa buku bacaan. Ini dimaksudkan untuk memberikan landasan teori yang kuat melalui buku-buku yang tersedia diperpustakaan, yang berhubungan dengan penulisan Laporan Skripsi ini.

I.5. Keaslian Penelitian

Berikut adalah tabel keaslian penelitian, penelitian mengenai pembelajaran penyandian data di dalam *database MySQL* menggunakan metode *vernam cipher* dan *gronsfeld cipher*.

Tabel I.1. Keaslian Penelitian

No	Nama / Tahun	Judul	Hasil Penelitian

1.	Azanuddin, 2013	Penyandian Short Message Service (SMS) Pada Telepon Selular Dengan Menggunakan Algoritma Gronsfeld	Dengan menerapkan algoritma gronsfeld dalam penyandian SMS, maka dapat mencegah dari ancaman penyadapan dan pencurian SMS karena SMS yang dikirim bukan berupa SMS yang asli melainkan berupa *chiperteks*, sehingga akan sulit untuk dimengerti penyerang.
2.	M. Sholeh Dan J.V. Hamokwarong, 2011	Aplikasi Kriptografi Dengan Metode Vernam Cipher Dan Metode Permutasi Biner	Aplikasi ini menggunakan dua metode enkripsi dan dekripsi agar lebih aman dan terjamin kerahasiaan data.
3.	Aman Julianto Pakpahan, 2013	Aplikasi Penyandian Data Dengan Menggunakan Algoritma Noekeon	Perangkat lunakyang dihasilkan diharapkan dapat menambah perbendaharaan aplikasi kriptografi
4.	Fachrul Rozi Pratama, 2016	Pembelajaran Penyandian Data Di Dalam Database MySQL Menggunakan Metode Vernam Cipher Dan Gronsfeld Cipher	Aplikasi ini menggunakan dua metode yang disatukan untuk menciptakan keamanan yang lebih dari satu metode.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam tugas akhir ini adalah 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 sstem 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, serta saran kepada perusahaan