BAB I

PENDAHULUAN

I.1. Latar Belakang

Basis Data banyak digunakan untuk menyimpan dan mengelola data-data dan informasi. Kebanyakan pengelola basis data tidak memperdulikan masalah keamanan. Padahal keamanan dalam sebuah basis data sangatlah penting, sebab para pencuri informasi dapat mencuri data-data di dalam basis data yang tidak memiliki keamanan. Basis data adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut. (Helmund, 2021 : 81). Masalah keamanan informasi yang bersifat penting atau rahasia tidak boleh diabaikan. Saat ini penyampaian informasi berbasis teks menjadi elemen yang paling umum digunakan dalam berkomunikasi. Berbagai tindakan penyalahgunaan informasi penting seperti pecurian, penyadapan, pemanfaatan bahakan modifikasi terhadap teks informasi yang didistribusikan masing sering terjadi, sehingga dapat merugikan pemillik informasi sendiri. Tindakan penyalahgunaan sering kali terjadi pada data yang didistribusikan melalui jaringan internet. (Hariati, dkk, 2018:13). Salah satu informasi yang harus diamankan adalah basis data. Penerapan keamanan pada basis data biasanya hanya menggunakan sandi *login* untuk melindungi isi di basis data. Akan tetapi jika basis data dicuri, maka pencuri dapat membuka isi datanya secara langsung menggunakan aplikasi basis data yang lain, sehingga pencuri dapat membaca isi

dari basis data yang dicuri. Oleh karena itu perlunya diterapkan keamanan dalam sebuah basis data sehingga para pencuri informasi tidak dapat mencuri data yang terdapat di dalam basis data dengan cara mengubah isi dari teks yang tersimpan di dalam basis data menjadi teks rahasia.

Teknik ini dikenal dengan kriptografi. Kriptografi ialah ilmu yang mempelajari bagaimana cara menjaga supaya pesan atau data tetap aman pada saat dikirimkan dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Kriptografi adalah ilmu dan seni untuk menjaga keamanan ketika pesan dikirim dari suatu tempat ke tempat lain. (Firdaus dan Waluyo, 2018 : 167). Namun untuk dapat merahasiakan isi teks basis data menggunakan teknik kriptografi dibutuhkan metode yang tepat sehingga mendapatkan hasil yang baik.

Berdasarkan penelitian yang dilakukan oleh Sari, dkk (2018) yang berjudul Analisa Algoritma Elgamal Dalam Penyandian Data Sebagai Keamanan *Database*, Sari, dkk menemukan adanya kelemahan elgamal dalam keamanan *database* yaitu penggunaan kunci bilangan prima dan tidak terdapat penambahan kunci dalam bentuk abjad.

Berdasarkan penelitian yang dilakukan oleh Erlianto dan Painem (2018) yang berjudul Aplikasi Kriptografi Pengamanan Database Menggunakan Metode AES Dan Vigenere Berbasis Desktop Pada Pada Divisi Pencegahan Dan Penanggulangan Hiv Aids Yayasan Kapeta, Erlianto dan Painem menemukan adanya kelemahan AES dan Vigenere dalam keamanan *database* yaitu proses metode AES yang panjang sehingga memberatkan proses enkripsi dan dekripsi.

Berdasarkan kedua penelitian yang menggunakan beberapa metode untuk kerahasiaan isi basis data dan menemukan kekurangan pada metode yang mereka gunakan, maka peneliti menggunakan metode *Zig-Zag Cipher* dan ROT13 untuk menutupi beberapa kelemahan yaitu dengan menggunakan metode *Zig-Zag Cipher* dan ROT13 tidak memberatkan proses enkripsi dan dekripsi dan metode *Zig-Zag Cipher* dan ROT13 memiliki kunci yang dapat menggunakan seluruh abjad. Dengan adanya metode *Zig-Zag Cipher* dan ROT13 maka basis data mendapatkan kerahasiaan isi teks yang lebih baik. Dengan latar belakang yang telah peneliti jelaskan maka peneliti menyimpulkan judul **"Impelementasi Metode *Zig-Zag Cipher* Dan ROT13 Untuk Kerahasiaan Data Pada Basis Data".**

I.2. Ruang lingkup Permasalahan

Ruang lingkup permasalahan yang dapat diberikan untuk penelitian ini adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Identifikasi masalah berdasarkan latar belakang yang telah dijelaskan di atas adalah sebagai berikut :

1. Basis data tidak memiliki kerahasiaan pada isi data yang tersimpan.
2. Terdapat kelemahan metode-metode yang digunakan pada peneliti sebelumnya dalam kerahasiaan basis data.
3. Belum terdapat aplikasi yang dapat merahasiakan isi teks basis data dengan metode *Zig-Zag Cipher* Dan ROT13.

I.2.2. Perumusan Masalah

Perumusan masalah pada penelitian ini yaitu :

1. Bagaimana menerapkan kerahasiaan isi teks pada sebuah data di dalam basis data ?
2. Bagaimana menerapkan metode *Zig-Zag Cipher* Dan ROT13 untuk kerahasiaan isi teks basis data ?
3. Bagaimana menghasilkan Aplikasi Implementasi Metode *Zig-Zag Cipher* Dan ROT13 Untuk Kerahasiaan Data Pada Basis Data ?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini berdasarkan latar belakang adalah sebagai berikut :

1. Aplikasi hanya untuk memberikan kerahasiaan isi teks pada basis data.
2. Aplikasi hanya dapat berjalan pada sistem operasi *windows*.
3. *Input* aplikasi ini berupa pesan teks pada isi basis data.
4. *Output* aplikasi ini berupa *ciphertext* dari isi basis data.
5. Pembuatan Aplikasi ini menggunakan bahasa pemrograman *Visual Basic* 2010.
6. Perancangan Aplikasi ini menggunakan pemodelan UML.
7. Metode yang digunakan adalah metode *zig-zag cipher* dan ROT13.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Menerapkan kerahasiaan isi teks pada sebuah data di dalam basis data.
2. Menerapkan metode *Zig-Zag Cipher* Dan ROT13 untuk kerahasiaan isi teks basis data.
3. Menghasilkan Aplikasi Implementasi Metode *Zig-Zag Cipher* Dan ROT13 Untuk Kerahasiaan Data Pada Basis Data.

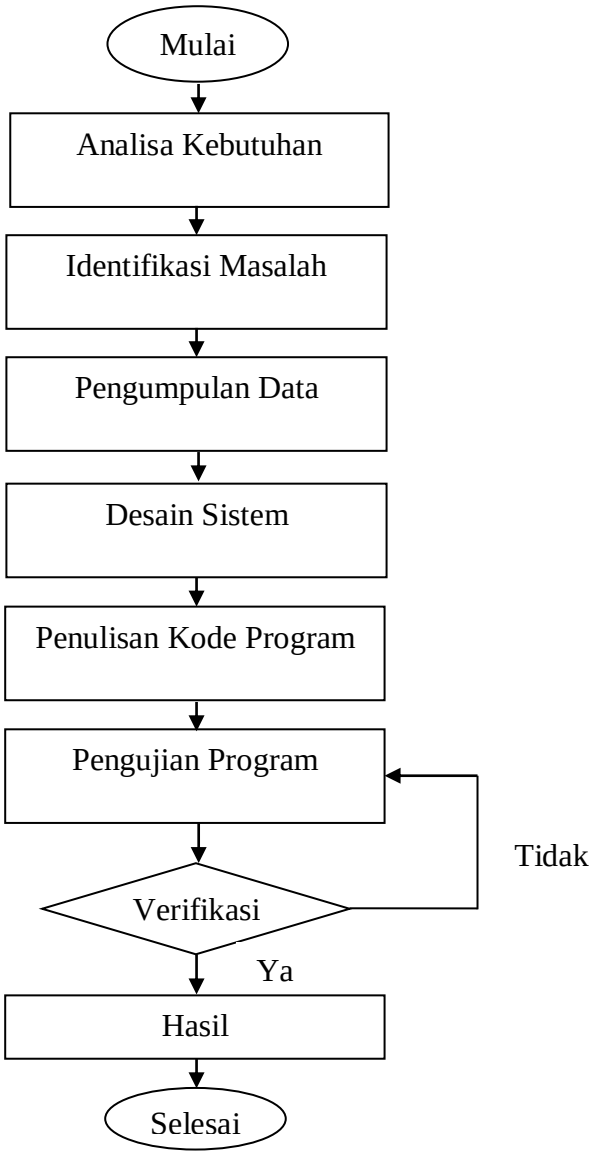
I.3.2. Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut :

1. Basis Data mendapatkan kerahasiaan yang lebih baik pada isi teksnya.
2. Mengetahui dan memahami implementasi metode *Zig-Zag Cipher* Dan ROT13 pada kerahasiaan isi teks basis data.
3. Mendapat wawasan dalam pembuatan aplikasi kriptografi.

I.4. Metodologi Penelitian

Penelitian ini akan melalui beberapa tahapan. Tahapan dalam penelitian ini dapat di modelkan pada *flowchart* sebagai berikut :



Gambar I.1. Diagram Alur Metode Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini peneliti mengumpulkan data-data yang berkaitan dengan penelitian dari Dinas Pendidikan. Peneliti juga menentukan *software* dan *hardware* yang akan digunakan untuk membuat penelitian. Berikut adalah data-data yang dibutuhkan :

a. Data Madrasah

b. Data Hasil Wawancara

Berikut adalah bahan bacaan yang digunakan untuk teori :

a. Buku

b. Jurnal

2. Identifikasi Masalah

Masalah yang teridentifikasi adalah basis data tidak memiliki kerahasiaan pada isi data yang tersimpan.

3. Pengumpulan Data

Peneliti melakukan pengumpulan data yang berkaitan dengan metode *zig-zag cipher,* ROT13 dan basis data.

4. Desain Sistem

Untuk mendesain sistem peneliti menggunakan beberapa pemodelan UML yaitu :

a. *Use case diagram*

Dengan menggunakan *use case diagram* maka peneliti dapat menggambarkan cara kerja aktor yang berkaitan dengan sistem sehingga dapat membentuk *class* dan *attribute.*

b. *Class diagram*

Dengan menggunakan *class diagram* maka peneliti dapat membuat struktur basis data yang akan digunakan.

c. *Activity diagram*

Dengan menggunakan *activity diagram* maka peneliti dapat menggambarkan aktifitas dari aktor pada sistem.

d. *Sequence diagram*.

Dengan *sequence diagram* maka peneliti dapat menggambarkan urutan penggunaan sistem untuk mengelola data.

5. Penulisan Kode Program

Dalam penulisan kode program, peneliti menggunakan bahasa pemrograman *Visual Basic* 2010 dengan menggunakan basis data sebagai penyimpanan data.

6. Pengujian Program

Pengujian program dilakukan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik. Pengujian dengan teori menggunakan *blackbox tesing* dan pengujian dengan praktek menggunakan *visual basic* 2010.

7. Hasil

Hasil yang diperoleh yaitu aplikasi implementasi metode *zig-zag cipher* dan ROT13 untuk kerahasiaan isi teks basis data.

I.6. Kontribusi Penelitian

Kontribusi yang dihasilkan penelitian ini yaitu :

Berdasarkan penelitian yang dilakukan oleh Sari, dkk (2018) yang berjudul Analisa Algoritma Elgamal Dalam Penyandian Data Sebagai Keamanan *Database*,

Sari, dkk menemukan adanya kelemahan elgamal dalam keamanan *database* yaitu penggunaan kunci bilangan prima dan tidak terdapat penambahan kunci dalam bentuk abjad.

Berdasarkan penelitian yang dilakukan oleh Erlianto dan Painem (2018) yang berjudul Aplikasi Kriptografi Pengamanan Database Menggunakan Metode AES Dan Vigenere Berbasis Desktop Pada Pada Divisi Pencegahan Dan Penanggulangan Hiv Aids Yayasan Kapeta, Erlianto dan Painem menemukan adanya kelemahan AES dan Vigenere dalam keamanan *database* yaitu proses metode AES yang panjang sehingga memberatkan proses enkripsi dan dekripsi.

Berdasarkan penelitian yang dilakukan oleh Hondro (2018) mengenai aplikasi enkripsi dan dekripsi sms dengan algoritma *zig zag cipher* pada *mobile phone* berbasis *android*, disimpulkan bahwa algoritma *zig zag cipher* dapat digunakan untuk enkripsi dan dekripsi sms pada perangkat *android*. Sedangkan penelitian penulis menggunakan metode *zig-zag cipher* untuk kerahasiaan isi teks basis data.

I.7. Sistematika Penulisan

Sistematika penulisan yang diajukan dalam skripsi 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 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.