BAB I

PENDAHULUAN

I.1. Latar Belakang

Basis Data digunakan untuk mengelola data-data dan informasi yang terdapat di dalam perangkat komputer ataupun *mobile*. Pada umumnya pengelola basis data tidak memperdulikan masalah kerahasiaan data yang terdapat di dalam basis data. Padahal kerahasiaan data dalam sebuah basis data sangatlah penting, sebab para pencuri informasi dapat mencuri data-data di dalam basis data yang tidak memiliki kerahasiaan data sehingga dapat digunakan untuk keperluan pribadi pencuri. Umumnya basis data hanya mengandalkan sandi login untuk akses ke dalam isi basis data. Akan tetapi isi basis data masih dapat terbaca oleh pihak yang tidak diinginkan yang mengetahui sandi *login* basis data. Masalah yang terjadi adalah kecurian isi dari basis data yang digunakan, sehingga merugikan pemilik basis data dan menguntungkan pencuri basis data untuk kepentingan pribadinya. Pencuri dapat diperoleh dari dua pihak yaitu pihak luar dan pihak dalam, pihak luar yaitu orang yang meretas isi basis data dari luar misalnya menggunakan SQL Injection dan pihak dalam dapat mencuri secara langsung isi basis data untuk dijual. Oleh karena itu dibutuhkan sebuah teknik yang dapat merahasiakan isi teks basis data dari pencuri informasi.

Peneliti merekomendasikan teknik kriptografi untuk merahasiakan isi dari basis data. Kriptografi penting dalam dunia teknologi informasi saat ini terutama dalam bidang komputer yang mempelajari teknik-teknik matematika yang

berhubungan dengan aspek keamanan informasi. Kriptografi juga menjadi salah satu syarat penting dalam keamanan teknologi informasi dalam melakukan pengiriman informasi ataupun data yang dianggap sangat penting dan rahasia. (Alam, dkk, 2019: 200). Dalam penggunaan kriptografi dibutuhkan sebuah metode untuk dapat mengubah isi pesan menjadi rahasia.

Contoh kasus pertama penyebab *database* yang tidak aman yaitu pengubahan *database* atau penyebab lainnya yang menyebabkan *database* dikatakan tidak aman.

Contoh kasus kedua penyebab *database* yang tidak aman yaitu adanya *hacker* yang menggunakan teknik SQL Injection dapat mencuri isi *database*.

Penelitian ini menggunakan metode *Porta Cipher* dengan memodifikasi kunci yang biasa digunakan *Porta Cipher* dan menggunakan *Diffie Hellman* untuk menggantikan penggunaan kunci pada *Porta Cipher*. Sehingga dengan adanya implementasi metode *Porta Cipher* dan *Diffie Hellman* maka basis data mendapatkan kerahasiaan data yang baik. Berdasarkan latar belakang tersebut maka peneliti menyimpulkan judul **"Metode Modifikasi *Porta Cipher* Dan *Diffie-Hellman* Untuk Kerahasiaan Isi Teks Basis Data Berbasis *Android*"**.

I.2. Ruang lingkup Permasalahan

Ruang lingkup permasalahan yang dijabarkan untuk penelitian ini adalah sebagai berikut:

I.2.1. Identifikasi Masalah

Identifikasi masalah dari latar belakang yang telah dijelaskan adalah sebagai

berikut:

1. Isi teks basis data tidak dirahasiakan sehingga dapat dicuri oleh pencuri informasi.
2. Belum ada modifikasi *porta cipher* dan *diffie hellman* untuk kerahasiaan basis data.
3. Belum ada aplikasi yang menggunakan modifikasi metode *porta cipher* dan *diffie hellman* untuk kerahasiaan basis data.

I.2.2. Perumusan Masalah

Perumusan masalah pada penelitian ini yaitu:

1. Bagaimana merahasiakan isi teks basis data dari pencuri informasi?
2. Bagaimana modifikasi *porta cipher* dan *diffie hellman* untuk kerahasiaan basis data?
3. Bagaimana menghasilkan aplikasi metode modifikasi *porta cipher* dan *diffie hellman* untuk kerahasiaan isi teks basis data berbasis *android*?

I.2.3. Batasan Masalah

Batasan masalah yang terdapat pada penelitian ini berdasarkan latar belakang yang telah dijabarkan adalah sebagai berikut:

1. Aplikasi hanya untuk merahasiakan isi basis data.
2. *Input* aplikasi ini berupa isi teks basis data.
3. *Output* aplikasi ini berupa isi teks basis data terenkripsi.
4. Aplikasi yang dirancang berbasis *android* menggunakan *eclipse juno*.

5. Perancangan Aplikasi ini menggunakan pemodelan UML.
6. *Database* yang digunakan adalah MySQL.
7. Merahasiakan isi basis data menggunakan perangkat *android*.
8. Metode yang digunakan adalah *porta cipher* dan *diffie hellman*.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Merahasiakan isi teks basis data dari pencuri informasi.
2. Memodifikasi *porta cipher* dan *diffie hellman* untuk kerahasiaan basis data.
3. Menghasilkan aplikasi metode modifikasi *porta cipher* dan *diffie hellman* untuk kerahasiaan isi teks basis data berbasis *android*.

I.3.2. Manfaat

Manfaat dari penelitian ini adalah sebagai berikut:

1. Isi teks yang terdapat di dalam basis data dapat dengan mudah dirahasiakan sehingga mendapatkan kerahasiaan data yang baik.
2. Mendapatkan pengetahuan mengenai metode *porta cipher* dan *diffie hellman* untuk kerahasiaan basis data.
3. Mendapatkan pengalaman dalam pembuatan aplikasi kriptografi.

I.4. Metodologi Penelitian

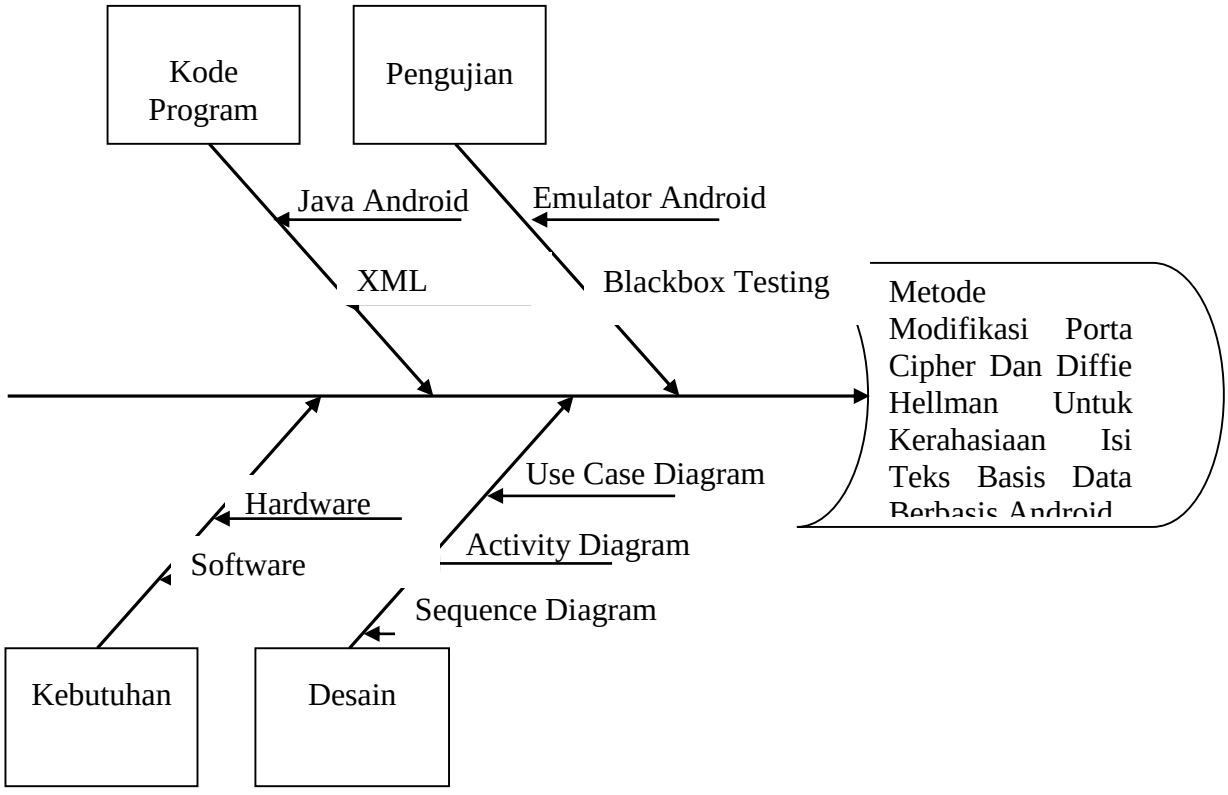
Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan dan adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut:

I.4.1. Pengumpulan Data

Pada tahapan ini peneliti menggunakan jurnal sebagai referensi dan landasan teori pada penelitian ini.

I.4.2. *Diagram Fish Bone*

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:



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

Keterangan:

1. Kebutuhan

Pada tahapan ini dilakukan pengumpulan untuk kebutuhan penelitian yaitu *hardware* dan *software*.

Pada tahapan ini peneliti menggunakan *software* dan *hardware* sebagai berikut:

a. *Software*

Software yang digunakan diantaranya:

1) Eclipse
2) Notepad
3) Appserve

b. *Hardware*

Hardware yang digunakan diantaranya:

1) Laptop
2) Perangkat *Android*

2. Kode Program

Kode program ditulis ke dalam bahasa pemrograman PHP dan *Java Android* yang berfungsi untuk mengendalikan cara kerja aplikasi dan HTML serta XML yang berfungsi sebagai pembuatan tampilan pada aplikasi yang dibuat.

3. Desain Sistem

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

a. *Use Case Diagram*

Use case diagram digunakan untuk menceritakan sistem yang berjalan sehingga mengetahui tahapan perancangan sistem selanjutnya.

b. *Activity Diagram*

Activity diagram digunakan untuk menggambarkan aktifitas pengguna terhadap sistem.

c. *Sequence Diagram*

Sequence diagram digunakan untuk menggambarkan urutan kerja pengguna terhadap sistem.

4. Pengujian

Pada tahapan ini peneliti menguji sistem yang telah dibuat menggunakan pengujian teori dan praktek. Pengujian teori peneliti menggunakan *blackbox testing* sebagai pencatatan hasil uji coba dari aplikasi dan pengujian praktek peneliti menggunakan *emulator* untuk menguji secara langsung penggunaan aplikasi.

5. Hasil

Pada tahapan ini penelitian sudah selesai dibuat, hasil dari penelitian ini yaitu Aplikasi Metode Modifikasi *Porta Cipher* Dan *Diffie Helman* Untuk Kerahasiaan Isi Teks Basis Data Berbasis *Android* dan apabila terjadi kekurangan pada aplikasi maka segera diperbaiki.

I.5. Kontribusi Penelitian

Berdasarkan penelitian yang dilakukan oleh (Al-omari, 2018) mengenai ABJAD *Arabic-Based Encryption*, Omari menggunakan metode *Porta Cipher* untuk merahasiakan abjad arab.

Berdasarkan penelitian yang dilakukan oleh (Saraswat et al., 2016) mengenai *An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication*, Saraswat, dkk menggunakan metode *Porta Cipher* untuk kerahasiaan komunikasi berbentuk teks.

Berdasarkan penelitian yang dilakukan oleh (Rosdiana, 2018) mengenai Rancang Bangun Aplikasi Penyandian Data Text Menggunakan Algoritma *Diffie-Hellman* Dan Algoritma RC4, Alam, dkk menggunakan metode *Diffie-Hellman* untuk pertukaran kunci RC4.

Berdasarkan penelitian yang dilakukan oleh (Khairani et al., 2021) mengenai Pengkodean *Monoalphabetic* Menggunakan *Affine Cipher* dengan Kunci *Diffie-Hellman*, Khairani, dkk menggunakan metode *Diffie-Hellman* untuk pertukaran kunci *Affine Cipher*.

I.6. 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, kontribusi 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.