BAB III
METODE PENELITIAN

3.1 Desain Penelitian

Pada bab ini dijelaskan skema umum penelitian yang akan dilakukan untuk memudahkan peneliti melakukan penelitian. Desain penelitian yang akan digunakan pada proses perancangan aplikasi *Instant Messaging* ini dapat dilihat pada gambar 3.1:

Gambar 3.1 Desain Penelitian

1.1.1 Identifikasi Masalah

Tahap ini merupakan tahap peneliti melakukan perumusan masalah dan menganalisis permasalahan yang akan diteliti. Permasalahan yang melatarbelakangi penelitian ini adalah karena maraknya pencurian data oleh pihak ketiga pada aplikasi *Instant Messaging*. Pada tahap ini juga peneliti menentukan algoritma kriptografi yang akan digunakan untuk mengamankan aplikasi *Instant Messaging* tersebut. Dalam penelitian ini peneliti menggunakan algoritma kriptografi Elgamal.

1.1.2 Studi Literatur

Tahap ini merupakan tahap peneliti mempelajari terkait dengan penelitian yang dilakukan yaitu mempelajari konsep *Instant Messaging*, mempelajari algoritma elgamal, mempelajari pemrograman android. Sumber yang digunakan oleh peneliti adalah buku, jurnal, skripsi dan informasi yang didapat dari internet.

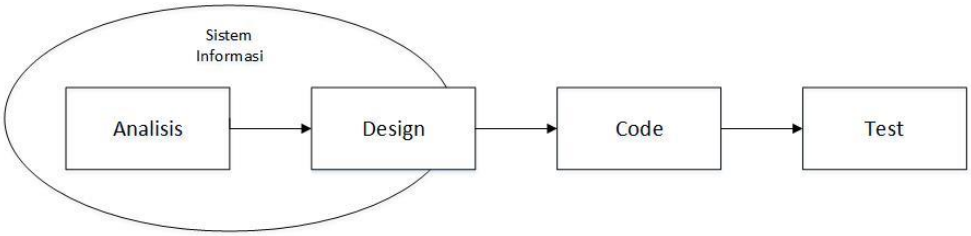
1.1.3 Perancangan Algoritma Elgamal

Pada tahapan ini peneliti melakukan perancangan algoritma elgamal yang langsung diterapkan pada platform Android. Perancangan yang dilakukan ialah dengan merancang proses pembangkitan kunci, proses enkripsi dan proses dekripsi. Dimana proses Algoritma Elgamal ini akan dilakukan secara otomatis oleh sistem.

Bahasa pemrograman yang digunakan dalam pembuatan algoritma Elgamal ini adalah Java Android.

1.1.4 Implementasi Algoritma pada Perangkat Lunak

Pada tahapan ini peneliti melakukan pembuatan perangkat lunak *Instant Messaging* yang dilengkapi sistem enkripsi algoritma Elgamal dengan menggunakan model proses *Sequential Linear* yang dikembangkan oleh Roger. Model ini merupakan model klasku yang bersifat sistematis yang memiliki langkah-langkah dalam membuat perangkat lunak. Setelah perangkat lunak dibuat maka selanjutnya mengimplementasikan algoritma elgamal pada perangkat lunak.



Gambar **Error! No text of specified style in document.**.2 Diagram Model *Sequential Linear* (Pressman.2002)

1.1.4.1 Analisis

Pada tahap ini, dilakukan pengumpulan data dan informasi yang diperoleh melalui observasi. Data yang didapat kemudian akan dianalisis apakah sudah sesuai dengan kebutuhan fungsional maupun non fungsional dalam pengamanan aplikasi *Instant Messaging.*

Kebutuhan fungsional yang dimaksud adalah kebutuhan yang meliputi pengguna aplikasi. Dimana pengguna dapat melakukan pengiriman pesan dalam keadaan aman tanpa perlu khawatir pesan nya akan diambil pihak ketiga.

Kebutuhan Non Fungsional yang dimaksud adalah kebutuhan yang meliputi performa keamanan yang digunakan pada aplikasi IM. Dimana proses keamanannya tidak memakan waktu yang lama sehingga tidak mengganggu aktivitas pengguna dalam menggunakan aplikasi.

1.1.4.2 Desain

Pada tahapan ini peneliti melakukan perancangan struktur data dengan menggunakan UML (*Unified Modeling Language*). Dengan menggunakan UML peneliti merancang struktur data dengan membuat *usecase, activity diagram, class diagram, object diagram, sequence diagram, collaboration diagram, component diagram,* dan *deployment diagram.*

1.1.4.3 Coding

Tahap ini merupakan tahap penerjemahan data atau pemecah masalah yang telah dirancang kedalam Bahasa pemrograman, peneliti menggunakan bahasa pemograman Java pada Android dan menggunakan bahasa matlab. Pengkodean terdiri dari pembuatan *user interface* aplikasi IM.

1.1.4.4 Testing

Merupakan tahap pengujian terhadap perangkat lunak yang dibangun yaitu sistem enkripsi *Instant Messaging* dengan menggunakan algoritma Elgamal secara menyeluruh dari desain antarmuka, alur, hingga fungsi-fungsi yang telah dirancang dapat dipastikan berjalan dengan baik dan benar. Fungsi utama yang akan menjadi fokus pengujian adalah pada proses pengiriman pesan pada IM dapat terenkripsi/terdekripsi dengan benar. Pada penelitian ini perangkat lunak akan memperlihatkan keamanan setelah dilakukan enkripsi dan bagaimana penerapan algoritma Elgamal tersebut pada IM.

1.2 Alat dan Bahan Penelitian

Berdasarkan kebutuhan-kebutuhan di atas, maka ditentukan bahwa alat dan bahan yang digunakan pada penelitian ini adalah sebagai berikut:

1.2.1 Alat Penelitian

Dalam penelitian ini, peneliti menggunakan bebagai alat bantu penunjang baik berupa perangkat keras maupun perangkat lunak. Adapun perangkat keras yang digunakan adalah seperangkat komputer yang mempunyai spesifikasi sebagai berikut:

1. Komputer
    a. Processor Intel Core 3
    b. RAM 4 GB
    c. Hardisk 500GB
2. Perangkat *Mobile* Android
    a. Xiaomi Redmi Note 5A Prime dengan OS Android

Sedangkan perangkat lunak yang digunakan yaitu :

1. Android Studio
2. Android SDK
3. Firebase

1.2.2 Bahan Penelitian

Bahan Penelitian yang digunakan berupa literature *textbook*, *paper*, tutorial, dan artikel yang didapat dari internet mengenai system enkripsi, *Instant Messaging*, kriptografi dan algoritma kriptografi Elgamal.