

# BAB I

## PENDAHULUAN

### I.1. Latar Belakang

Salah satu bentuk komunikasi berbasis teks yang banyak digunakan di *social media* adalah aplikasi *messenger*. Layanan *web* seperti *facebook* dan *yahoo* juga menyediakan fasilitas *messenger* untuk berkirim pesan dengan menggunakan jaringan *internet*. Aplikasi *messenger* banyak dilakukan karena penggunaannya yang relatif mudah, serta dalam keadaan yang sibuk masih tetap dapat memanfaatkan aplikasi tersebut. Pesan yang dikirimkan antar pengguna aplikasi *messenger* perlu diberikan layanan keamanan data, sehingga hanya orang-orang yang memiliki otoritas saja yang dapat mengetahui isi pesan yang disampaikan tersebut. Perlu dibuat mekanisme supaya pesan yang dikirimkan dapat terjaga kerahasiaannya.

Salah satu ilmu pengamanan data yang terkenal adalah kriptografi yang merupakan 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*). Terdapat beberapa *algoritma* dalam kriptografi, algoritma yang digunakan dalam penelitian ini adalah ROT 13 dan *One Time Pad* (OTP).

Rot 13 (*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. Sedangkan OTP adalah *stream cipher* yang melakukan enkripsi dan dekripsi satu karakter setiap kali. *Algoritma* ini ditemukan pada tahun 1917 oleh Major Joseph Mauborgne sebagai perbaikan dari *vernam cipher* untuk menghasilkan keamanan yang sempurna. Alasan digunakannya *algoritma* OTP (*One Time Pad*) adalah karena dalam segi keamanannya yang baik, selain itu *algoritma* OTP (*One Time Pad*) juga ringan, cepat serta memiliki kompatibilitas yang baik.

Untuk membangun sebuah aplikasi *messenger* yang dapat digunakan secara *real time* dalam penelitian ini akan digunakan layanan *database* yang telah disediakan oleh Google yang bernama *Firebase*. Oleh sebab itu, penulis akan mencoba memecahkan permasalahan keamanan pada aplikasi *messenger* dengan menerapkan *algoritma* kriptografi, sehingga pengguna tidak perlu takut untuk bertukar pesan yang bersifat rahasia. Berdasarkan latar belakang diatas, maka pada skripsi ini akan ditarik sebuah judul “**Implementasi Algoritma ROT 13 dan One Time Pad (OTP) Dalam Aplikasi Real Time Mesenger Berbasis Android**”.

## **I.2. Ruang Lingkup Permasalahan**

### **I.2.1. Identifikasi Masalah**

Adapun hal-hal yang menjadi identifikasi masalah dalam penelitian ini adalah :

1. Aplikasi *messenger* yang ada saat ini tidak dapat mengirimkan pesan dalam bentuk cipherteks.
2. Dibutuhkan penggabungan algoritma ROT 13 dan OTP untuk menghasilkan keamanan yang lebih baik.
3. Dibutuhkan sebuah aplikasi yang dapat mengirimkan pesan secara *real time* dengan kemampuan untuk mengamankan pesan yang akan dikirim.

### **I.2.2. Perumusan Masalah**

Berikut penulisan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini, antara lain :

1. Bagaimana membangun sebuah aplikasi *real time messenger* untuk digunakan pada *smartphone* android ?
2. Bagaimana menerapkan *algoritma* ROT 13 dan OTP untuk mengamankan pesan yang dikirimkan melalui aplikasi *messenger* ?
3. Bagaimana penggunaan *database* dalam pengelolaan data dari sebuah aplikasi *real time messenger* ?

### **I.2.3. Batasan Masalah**

Dalam penulisan skripsi ini dibatasi permasalahannya sebagai berikut :

1. Aplikasi ini dibangun untuk digunakan pada *smartphone* android sebagai sebuah media untuk bertukar pesan teks secara rahasia.
2. Algoritma yang digunakan untuk mengamankan pesan adalah algoritma ROT-13 dan algoritma OTP.

3. Bahasa pemrograman yang digunakan untuk membangun aplikasi pada penelitian ini adalah Java.
4. Perangkat lunak yang akan digunakan dalam membangun aplikasi media pembelajaran pengenalan gunung berapi di Indonesia adalah Android Studio.
5. Perancangan aplikasi dibuat menggunakan *Unified Modeling Language* (UML) seperti *use case*, *activity diagram* dan *sequence diagram*.

### **I.3. Tujuan dan Manfaat**

#### **I.3.1. Tujuan**

Tujuan yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut :

1. Menghasilkan sebuah aplikasi *real time messenger* untuk digunakan pada *smartphone* android.
2. Menerapkan *algoritma* ROT 13 dan OTP untuk mengamankan pesan yang akan dikirim melalui aplikasi *messenger*.
3. Menghasilkan sebuah sistem pertukaran pesan yang dapat dijadikan sebagai media dalam bertukar pesan rahasia secara aman.

#### **I.3.2. Manfaat**

Adapun manfaat yang dapat diambil dalam penulisan skripsi ini adalah:

1. Dapat digunakan oleh pengguna aplikasi untuk bertukar pesan menggunakan *smartphone* android.

2. Dengan menerapkan *algoritma* ROT 13 dan OTP dapat dijadikan sebagai media bertukar pesan yang aman.
3. Hasil penelitian dapat dijadikan referensi bagi peneliti lain yang akan melakukan penelitian tentang mengamankan pesan.

#### **I.4. Metodologi Penelitian**

Untuk dapat mengimplementasikan sistem di atas, maka secara garis besar digunakan beberapa metode sebagai berikut:

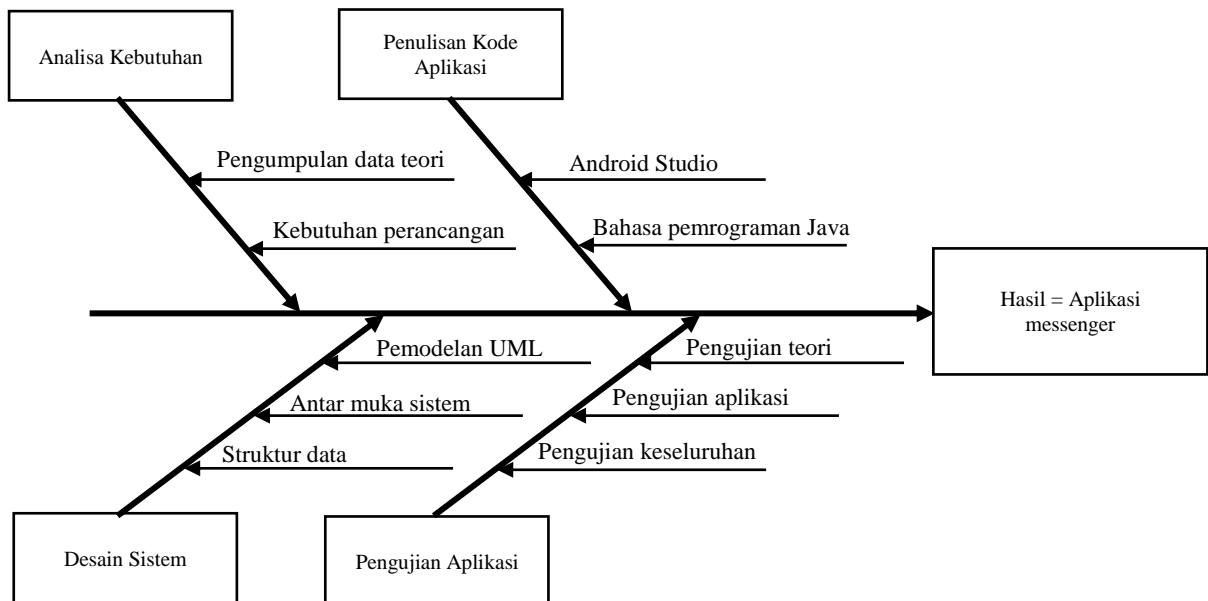
##### **I.4.1. Metode Pengumpulan Data**

Sistem yang dirancang tentunya memerlukan pengumpulan data, dalam proses pengumpulan data terdapat beberapa cara, berikut diantaranya :

1. Studi Literatur, dengan cara mempelajari buku-buku acuan dan literatur yang berhubungan dengan materi dalam penulisan skripsi. Buku-buku acuan yang digunakan umumnya adalah tentang cara penyusunan skripsi pada Universitas Potensi Utama dan juga buku-buku tentang studi pustaka yang digunakan dalam penulisan skripsi.
2. *Internet*, yaitu penulis mencari data-data yang mendukung penulisan skripsi melalui *internet*. Dalam penulisan skripsi ini penulis mencari jurnal-jurnal yang dijadikan acuan melalui *internet*. Jurnal yang dicari melalui *internet* dapat berupa jurnal nasional maupun internasional.

### I.4.2. Metode Perancangan Sistem

Langkah-langkah yang diperlukan untuk mencapai tujuan perancangan dapat dilihat pada *diagram fishbone* gambar I.1.



**Gambar I.1. Diagram Fishbone Prosedur Perancangan**

#### 1. Analisis Kebutuhan

Setelah melalui tahap prosedur perancangan, maka tahap selanjutnya adalah analisa kebutuhan yaitu hal-hal yang diperlukan untuk perancangan sistem berupa perangkat lunak yaitu Android Studio yang digunakan untuk merancang aplikasi untuk perangkat android dan perangkat keras seperti komputer atau laptop yang dibutuhkan untuk membangun aplikasi. *Smartphone* android juga dibutuhkan dalam proses uji coba aplikasi.

## 2. Desain Sistem

Pada tahap ini dirancang sebuah desain dari perancangan aplikasi implementasi algoritma ROT 13 dan One Time Pad (OTP) dalam aplikasi *real time mesenger* berbasis android. Bagaimana desain yang akan digunakan pada antarmuka perangkat berbasis android Setelah dilakukan perancangan desain aplikasi selanjutnya melakukan implementasi terhadap desain antarmuka dari aplikasi berbasis android yang telah dirancang kedalam bahasa pemrograman JAVA.

## 3. Penulisan Kode Aplikasi

Pada proses ini perancangan aplikasi implementasi algoritma ROT 13 dan One Time Pad (OTP) dalam aplikasi *real time mesenger* berbasis android dituangkan kedalam bahasa pemrograman java dan mulai dibangun menggunakan perangkat lunak android studio untuk menghasilkan sebuah aplikasi sesuai dengan perancangan. Seluruh fungsi dan antarmuka yang terdapat pada perancangan akan disesuaikan dengan aplikasi yang akan dihasilkan.

## 4. Pengujian Aplikasi

Pada tahap ini dilakukan pengujian aplikasi implementasi algoritma ROT 13 dan One Time Pad (OTP) dalam aplikasi *real time mesenger* berbasis android secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan aplikasi. Pengujian fungsional dilakukan untuk mengetahui bahwa aplikasi implementasi algoritma ROT 13 dan One Time Pad (OTP) dalam aplikasi *real time mesenger* berbasis android telah berjalan dengan sesuai dengan perancangan. Pengujian ketahanan merupakan kemampuan aplikasi untuk berjalan

dengan baik pada spesifikasi minimum komputer.

## 5. Hasil

Pada tahap ini akan diambil kesimpulan dari aplikasi implementasi algoritma ROT 13 dan One Time Pad (OTP) dalam aplikasi *real time mesenger* berbasis android yang telah dihasilkan, seperti apa saja kelebihan dan kekurangan dari aplikasi implementasi algoritma ROT 13 dan One Time Pad (OTP) dalam aplikasi *real time mesenger* berbasis android. Sehingga didapatkan kesimpulan untuk menambahkan fungsi-fungsi tertentu sesuai dengan kebutuhan kedalam aplikasi.

### **I.5. Kontribusi Penelitian**

Adapun kontribusi yang diberikan pada penelitian yang dilaksanakan adalah berupa :

1. Aplikasi ini dapat digunakan untuk berkomunikasi dalam bentuk pesan teks menggunakan *smartphone* android.
2. Aplikasi ini dapat digunakan sebagai media dalam bertukar pesan yang bersifat rahasia.

### **I.6. Sistematika Penulisan**

Adapun sistematika penulisan yang diajukan dalam penulisan skripsi ini adalah sebagai berikut :

**BAB I : PENDAHULUAN**

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

**BAB II : TINJAUAN PUSTAKA**

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

**BAB III : ANALISA DAN DESAIN SISTEM**

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

**BAB IV : HASIL DAN UJI COBA**

Pada bab ini menerangkan hasil dan pembahasan aplikasi yang dirancang serta kelebihan dan kekurangan aplikasi yang dirancang.

**BAB V : KESIMPULAN DAN SARAN**

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk pembuatan aplikasi implementasi algoritma ROT 13 dan *One Time Pad* (OTP) dalam aplikasi *real time mesengger* berbasis android.