BAB I

PENDAHULUAN

I.1. Latar belakang

“ Android adalah salah satu alat komunikasi yang umum digunakan oleh sebagian masyarakat untuk pertukaran informasi dan mengirimkan pesan.” *Android* menyediakan media untuk melakukan komunikasi pertukaran pesan yaitu aplikasi *chatting*. Pertukaran pesan melalui *chatting* ini sangat popular penggunaannya di kalangan masyarakat dikarenakan begitu mudah tanpa khawatir jarak dan waktu.

Meskipun kebutuhan untuk bertukar pesan sekarang ini sudah sangat mudah, namun bukan berarti hal tersebut tidak memiliki kekurangan. Jika tidak diamankan sebelum diterima, pesan bisa saja di akses oleh orang yang tidak bertanggung jawab selama masa pengiriman.

Padahal hal tersebut dapat dihindari dengan cara merahasiakan pesan atau informasi sehingga hanya dapat dipahami oleh orang-orang tertentu. Teknik untuk merahasiakan pesan ini dikenal dengan nama *Kriptografi.*

Kriptografi berasal dari bahasa Yunani dengan memadukan dua kata, yaitu *kryptos* dan *graphein*. *Kryptos* berarti tersembunyi atau rahasia, sedangkan *graphein* memiliki arti menulis. Maka “*kriptografi* adalah menulis secara tersembunyi untuk menyampaikan pesan-pesan yang perlu dijaga kerahasiaanya.”

Kriptografi sendiri memiliki dua konsep yang penting, yaitu enkripsi dan dekripsi. “Enkripsi adalah salah satu teknik mengubah informasi atau data menjadi bentuk yang hampir tidak dikenali seperti informasi awal menggunakan algoritma tertentu”, sedangkan “Dekripsi adalah mengubah bentuk tersamar tersebut menjadi informasi awal.

Salah satu algoritma yang dapat diterapkan dalam mengamankan pesan adalah *ROT* 13 (*Roll Over Test*) dan *Vigenere Cipher*. “ Algoritma *ROT* 13 (*Roll Over Test*) yaitu algoritma enkripsi sederhana dari *Caesar Cipher* dengan geseran 13.”. Sedangkan “Algoritma *Vigenere Cipher* adalah menyembunyikan pesan berupa teks melalui teknik substitusi dengan mengubah setiap huruf menjadi huruf lain berdasarkan tabel kunci yang digunakan”. Algoritma ini melakukan pengamanan dengan mengacak pesan sehingga apabila pesan yang disampaikan bersifat pribadi atau hanya ingin diketahui oleh user tertentu, pesan tersebut tidak dapat untuk dimengerti dan juga kerahasiaan pesan asli dapat terjaga dengan aman.

Penerapan kombinasi dari kedua algoritma di atas diharapkan mampu meningkatkan keamanan dari sebuah pesan sebelum dikirimkan kepada penerima melalui aplikasi *chatting*, serta menjadi aplikasi alternatif yang digunakan masyarakat dalam bertukar pesan atau informasi. Berdasarkan penjelasan di atas, penulis tertarik untuk mengangkat penelitian berjudul **“Implementasi Algoritma *ROT* 13 dan *Vigenere Cipher* dalam pesan pada aplikasi *chat* berbasis *Android*”**

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Sehubungan dengan permasalahan yang ada maka penulis mencoba untuk mengidentifikasi masalah adalah :

1. Jika tidak diamankan sebelum diterima, pesan bisa saja diakses oleh orang yang tidak bertanggung jawab selama masa pengiriman.
2. Pengiriman pesan yang di sandikan menggunakan algoritma kriptografi masih rentan menimbulkan kecurigaan dalam masa pengiriman.
3. Dibutuhkan mekanisme pengamanan tambahan terhadap pesan yang sudah disandikan dengan kriptografi.

I.2.2. Perumusan Masalah

Rumusan masalah pada penelitian ini yaitu :

1. Bagaimana mengamankan pesan selama pengiriman?
2. Bagaimana menerapkan algoritma *Rot* 13 dan *Vigenere Cipher* dalam mengamankan pesan?
3. Bagaimana mengimplementasikan algoritma *Rot* 13 dan *Vigenere Cipher* dalam aplikasi *chatting*?

I.2.3. Batasan Masalah

Adapun batasan masalah dari penelitian ini yaitu :

1. Perancangan dan pembangunan aplikasi hanya sebatas untuk pengguna sistem operasi *android.*
2. Pengamanan hanya terhadap pesan teks.
3. Metode yang akan dipakai dalam penyelesaian masalah pengamanan pesan *chatting* adalah algoritma *Rot* 13 dan *Vigenere Cipher.*
4. Karakter yang dapat di *enkripsi* hanya huruf.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penelitian ini yaitu :

1. Mengamankan pesan sebelum diterima kepada penerima.
2. Menerapkan algoritma *Rot* 13 dan *Vigenere Cipher* dalam mengamankan pesan.
3. Mengimplementasikan algoritma *Rot* 13 dan *Vigenere Cipher* dalam aplikasi *chatting*.

I.3.2. Manfaat

Adapun manfaat dari penelitian ini yaitu :

1. Agar dapat memahami bagaimana pengamanan pesan *chatting* dengan menggunakan algoritma *Rot* 13 dan *Vigenere Cipher.*
2. Memberikan keamanan dalam melakukan pengiriman pesan.

I.4. Metodologi Penelitian

I.4.1. Pengumpulan Data

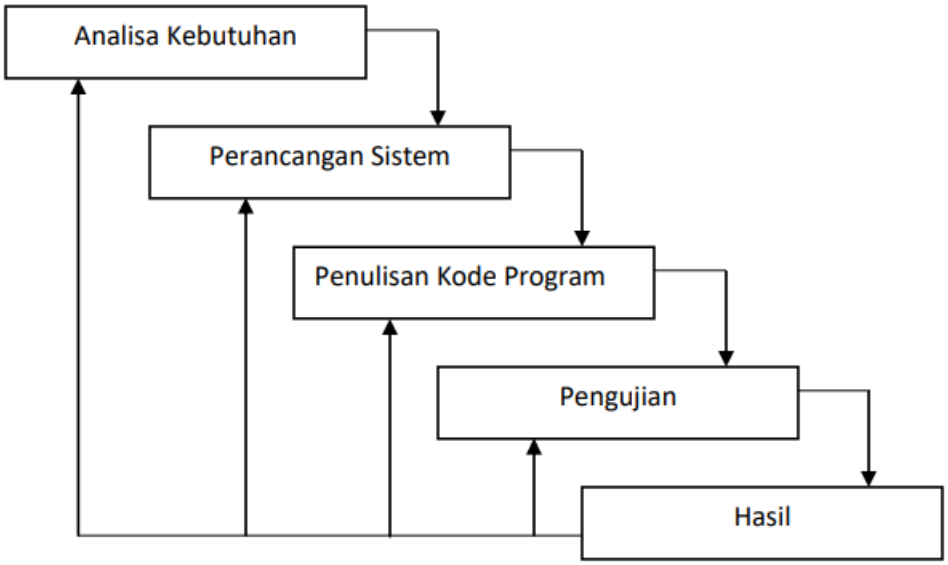
Pada tahap ini dilakukan dengan mempelajari teori dasar yang mendukung penelitian, pencarian dan pengumpulan data-data yang dibutuhkan. Untuk mengumpulkan data yang dibutuhkan, maka penulis menggunakan teknik :

1. **Tinjauan Pustaka (*Library Research*)**

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

I.4.2. Metode Perancangan Sistem

Tahapan dalam penelitian ini dapat di modelkan dengan *Waterfall* metodologi penelitian. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :



Gambar I. 1. Diagram *Waterfall*

Keterangan :

1. **Analisa Kebutuhan**

   Peneliti menganalisis kebutuhan untuk perancangan sistem berupa perangkat lunak yaitu *Android Studio* yang digunakan untuk merancang aplikasi sertaa perangkat keras seperti laptop untuk membangun sebuah aplikasi.

2. **Perancangan Sistem**

Pada tahap ini peneliti merancang sebuah desain dari aplikasi pengamanan pesan *chatting* dengan menggunakan algoritma *Rot* 13 dan *Vigenere Cipher*. Serta menggunakan pemodelan UML yaitu *use case diagram, class diagram, activity diagram, dan Sequence diagram* untuk perancangan sistem.

3. **Penulisan Kode Program**

Pada proses pengamanan aplikasi *chatting*, peneliti menggunakan metode *Rot* 13 dan *Vigenere Cipher* dengan menggunakan bahasa *Java* pada aplikasi *Android Studio.*

4. **Pengujian**

Pada tahap ini peneliti melakukan pengujian aplikasi pengamanan pesan pada aplikasi *chatting* dengan Algoritma *Rot* 13 dan *Vigenere Cipher* secara keseluruhan. Seperti pengujian fungsional dan pengujian kemampuan aplikasi dalam mengamankan pesan apakah sudah berjalan dengan baik.

5. **Hasil**

Pada tahapan ini peneliti telah menyelesaikan seluruh penelitian baik teori maupun aplikasi yaitu Implementasi Algoritma *Rot* 13 dan *Vigenere Cipher* dalam pesan pada aplikasi *chat* berbasis *Android*.

I.5. Kontribusi Penelitian

Adapun kontribusi penelitian ini adalah :

Berdasarkan penelitian yang dilakukan oleh (Sahara, 2018) dengan judul "Implementasi Pengamanan Pesan *Chatting* menggunakan Metode *Vigenere Cipher* dan *Cipher Block Chainning*" Tujuan penelitian ini yaitu merancang sebuah

aplikasi *online* sistem berbais *web* dalam mengamankan pengiriman pesan *chatting*. Dengan adanya aplikasi ini, masyarakat (Pengguna pesan *chatting*) mampu mengirimkan pesan kepada *user* lain dengan tenang tanpa khawatir isi pesan diketahui oleh orang lain.

Adapun perbedaan penelitian yang dilakukan penulis dengan penelitian terkait sebelumnya yaitu pada penelitian ini penulis menggunakan aplikasi berbasis *Android* untuk melakukan penngiriman pesan *chatting*. Sehingga dengan adanya aplikasi ini, dapat memberikan rasa aman kepada masyarakat (pengguna aplikasi *chatting*) atau *user* lainnya dalam melakukan pengiriman pesan *chatting*.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam penelitian 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 tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi yaitu berupa pembahasan mengenai sistem keamanan, *UML* dan normalisasi.

BAB III : ANALISIS DAN PERANCANGAN

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 program yang dirancang serta kelebihan dan kekurangan sistem 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 system.