BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi yang pesat berdampak pada cara manusia dalam berkomunikasi dan memperoleh informasi. Peristiwa ini dapat dirasakan dengan melihat ragam media komunikasi yang tersedia di lingkungan sosial. *Short Message Service (SMS)* merupakan salah satu jenis media komunikasi pesan teks yang kini mulai ditinggalkan. Menurut Church dan Oliveira (2013), pengaruh sosial adalah salah satu penyebab utama orang-orang bermigrasi untuk mulai menggunakan *Mobile Instant Messaging*, namun *Mobile Instant Messaging* tidak dapat mengganti keseluruhan fungsi *SMS* sebab dalam kondisi tertentu pengguna menganggap *SMS* sebagai jenis komunikasi yang lebih menjaga privasi, lebih formal, dan umumnya dapat diandalkan.

SMS merupakan layanan berbayar yang tersedia pada perangkat telepon seluler muncul sejak tahun 1993. Penggunaan yang mudah serta biaya yang relatif murah tetap menjadikannya sebagai salah satu pilihan pengguna dalam komunikasi via pesan teks. Namun peristiwa tersebut dianggap belum cukup untuk beberapa pengguna yang menginginkan jaminan atas kerahasiaan pesan mereka. Oleh sebab itu, peneliti berpendapat bahwa keamanan adalah aspek penting yang sebaiknya diimplementasikan kedalam *SMS* guna meningkatkan keamanan dan merahasiakan komunikasi yang berlangsung via pesan teks. Hal tersebut dapat diwujudkan dengan menambahkan kriptografi sebagai fitur

tambahan aplikasi pengelola layanan pesan singkat (*SMS*). Dengan adanya kriptografi, seorang pengirim dapat menyandikan teks pesan sebelum dikirim, sehingga teks pesan akan diterima dalam bentuk kode yang harus diterjemahkan terlebih dahulu untuk mengetahui isi pesan.

Kriptografi merupakan bidang ilmu penyandian yang memiliki berbagai metode dalam penerapannya. Adapun metode yang digunakan dalam penelitian ini adalah metode algoritma *Hill Cipher* dan algoritma *Vigenere Cipher*. Algoritma tersebut dipilih berdasarkan keunggulan yang ada yaitu, *Hill Cipher* memiliki resistensi terhadap analisis frekuensi sedangkan *Vigenere Cipher* membuat kriptanalis merasa sulit karena huruf yang sama dalam *chipertext* belum tentu huruf yang sama dalam *plaintext* (Sumandri, 2017).

Berdasarkan latar belakang tersebut, maka peneliti memilih **Implementasi Kriptografi Pesan Singkat (*SMS*) Dengan Algoritma Hill Cipher Dan Vigenere Cipher Berbasis Android** sebagai subjek penelitian dan judul skripsi. Dalam penelitian ini akan dirancang sebuah aplikasi ponsel pintar yang berbasis sistem operasi *Android*.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah yang peneliti temukan pada penelitian ini adalah sebagai berikut:

1. Pesan *SMS* bersifat pribadi namun belum memiliki keamanan teks.

2. Dibutuhkan sebuah aplikasi yang dapat menyandikan pesan teks menggunakan metode algoritma *Hill Cipher* dan *Vigenere Cipher*.
3. Dibutuhkan perancangan dan pembangunan aplikasi berbasis android untuk mengamankan komunikasi pesan teks via *SMS.*

I.2.2. Perumusan Masalah

Berdasarkan identifikasi masalah tersebut, maka dirumuskan masalah sebagai berikut:

1. Bagaimana mengamankan komunikasi pesan teks via *SMS.*
2. Bagaimana penggunaan metode algoritma *Hill Cipher* dan algoritma *Vigenere Cipher* dalam menyandikan pesan teks.
3. Bagaimana merancang dan membangun aplikasi yang mengamankan komunikasi *SMS* berbasis android menggunakan Java dan Android Studio.

I.2.3. Batasan Masalah

Adapun batasan masalah yang peneliti buat pada penelitian ini agar pembahasan pada penelitian ini tidak terlalu luas cakupannya ialah sebagai berikut:

1. Aplikasi ini dibangun untuk digunakan sebagai alat penyandian pesan teks yang akan dikirim.
2. Karakter teks yang digunakan terbatas pada *ASCII Printable Characters*.
3. Algoritma yang digunakan untuk menyandikan pesan adalah *Hill Cipher* dan *Vigenere Cipher* dan tidak membandingkan kedua algoritma.

4. Jumlah karakter pada kunci yang digunakan untuk proses menyandikan pesan sebanyak 4 atau 9 karakter.
5. IDE yang digunakan pada aplikasi adalah Android Studio.
6. Bahasa pemrograman yang digunakan adalah bahasa pemrograman Java.
7. Perancangan aplikasi dimodelkan menggunakan *Unified Modeling Language* (*UML*) seperti *usecase diagram*, *activity diagram* dan *sequence diagram*.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

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

1. Untuk mengamankan pesan teks yang besifat pribadi sebelum dikirim melalui *SMS*.
2. Untuk menyandikan pesan teks menggunakan metode algoritma *Hill Cipher* dan *Vigenere Cipher*.
3. Untuk merancang dan membangun aplikasi berbasis android yang dapat mengamankan komunikasi via pesan teks.

I.3.2. Manfaat

Adapun manfaat yang akan diperoleh dalam penulisan skripsi ini adalah sebagai berikut:

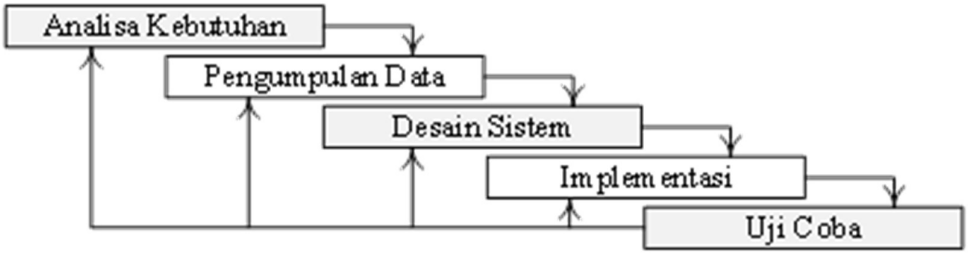
1. Menambah pengetahuan dan wawasan penulis mengenai konsep dan metode kerja algoritma *Hill cipher* dan *Vigenere cipher.*

2. Sebagai solusi untuk pengguna yang ingin mengamankan komunikasi pesan teks via *SMS*.
3. Sebagai bahan referensi bagi peneliti yang ingin membahas topik yang terkait dalam penelitian ini.

I.4. Metodologi Penelitian

Metodologi sistem perangkat lunak telah mengenalkan beberapa model yang dapat digunakan sebagai pendekatan dalam penelitian di bidang ilmu komputer. Secara garis besar model tersebut merangkum beberapa hal yaitu persyaratan elisitasi, desain sistem, implementasi, pengujian dan verifikasi (Turner, 2018). Adapun pengembangan aplikasi dalam penelitian ini akan menggunakan model *waterfall* karena model ini baik digunakan ketika memiliki persyaratan kebutuhan yang jelas.

Waterfall merupakan model pengembangan sistem yang bersifat linier. Saqib Saeed, et al. (2014) menjelaskan bahwa model ini menekankan pada perencanaan dan dokumentasi intensif sehingga kita mampu mengidentifikasi cacat desain sebelum pengembangan. Model *waterfall* yang paling sederhana terdiri dari fase yang tumpang tindih dimana setiap fase "mengalir" ke fase berikutnya. Terdapat beberapa variasi dalam model *waterfall* sederhana. Satu yang paling penting adalah dengan fungsi koreksi dimana cacat yang terdeteksi dikoreksi dengan kembali ke fase yang sesuai.



Gambar I.1. Kerangka Kerja Model Waterfall

1. Analisa Kebutuhan *(Requirments Analysis)*, pada tahap ini dilakukan analisis terhadap rumusan masalah dan batasan yang ada dalam skripsi ini. Analisis ini juga dilakukan untuk menganalisis spesifikasi sistem yang akan dibuat sesuai dengan batasan yang ada.
2. Pengumpulan Data *(Data Collection)*, dilakukan untuk memperoleh informasi yang dibutuhkan dalam rangka mencapai tujuan penelitian. Data yang dikumpulkan dengan menggunakan metode berikut..
    a. Studi literatur, penulisan ini dimulai dengan studi kepustakaan, yaitu dengan mengumpulkan bahan-bahan referensi dari jurnal, buku, ataupun berbagai sumber lain yang mendukung pembuatan aplikasinya.
    b. Metode wawancara, melakukan wawancara kepada pihak yang bersangkutan seperti mahasiswa dan pekerja swasta mengenai perancangan aplikasi yang berjalan sehingga nantinya aplikasi ini dapat digunakan.
    c. Metode observasi, melakukan pengamatan langsung bagaimana penggunaan *SMS* serta keamanannya untuk mengetahui langkah-langkah yang perlu diambil dalam perancangan aplikasi ini.

3. Desain Sistem *(System Design)*, pada tahap ini dilakukan proses perancangan desain sistem berdasarkan hasil analisis kebutuhan dan pengumpulan data. Pada tahap perancangan ini dilakukan beberapa perancangan yaitu perancangan arsitektur sistem, perancangan antarmuka, perancangan modul lainnya yang akan berintegrasi dalam suatu sistem.
4. Implementasi *(Implementation)*, Pada tahap ini dilakukan pengembangan sistem yang dibangun berdasarkan masukan dari desain sistem, pengembangan sistem dilakukan kedalam program kecil yang disebut sebagai unit, yang terintegrasi pada tahap selanjutnya. Setiap unit dikembangkan dan diuji fungsinya, yang kemudian disebut sebagai unit *testing.*
5. Uji Coba *(Testing)*, Semua unit yang telah dikembangkan pada tahap implementasi dirintegrasikan kedalam sistem setelah pengujian setiap unit kemudian seluruh sistem diuji untuk menemukan setiap kesalahan dan kegagalan. Uji coba dilakukan dengan memasukkan data pengujian tertentu, untuk melihat kesiapan sistem di dunia nyata.

I.5. Kontribusi Penelitian

Penelitian ini diharapkan dapat memberikan maanfaat dari sisi keilmuan tentang pemahaman cara kerja algoritma *Hill cipher* dan *Vigenere cipher* dengan mengimplementasikan kriptografi pesan singkat (*SMS)* dengan algoritma *Hill Cipher* dan *Vigenere Cipher* kedalam perangkat berbasis *Android*. Tidak hanya itu aplikasi ini juga diharapkan sebagai media pembelajaran tentang kriptografi yang telah menjadi kebutuhan layanan keamanan.

I.6. Sistematika Penulisan

Untuk mempermudah peneliti dalam penyusunan skripsi agar lebih singkat dan terstruktur, maka sistematika penulisan ini adalah sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini menguraikan hal-hal yang menjadi dasar latar belakang pelaksanaan skripsi, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi dan sistematika penulisan skripsi.

BAB II: TINJAUAN PUSTAKA

Pada bab ini menjelaskan tentang landasan teori, pengertian *SMS*, kriptografi, algoritma *Hill Cipher* dan *Vigenere Cipher*.

BAB III: ANALISIS DAN DESAIN SISTEM

Pada bab ini menjelaskan tentang analisis algoritma *Hill Cipher* dan *Vigenere Cipher* pada aplikasi *SMS* serta rancangan program yang akan dibuat berdasarkan masalah yang ada dan berisikan tentang bagaimana program itu dikembangkan.

BAB IV: HASIL DAN UJI COBA

Bagian ini menguraikan tentang hasil sistem yang dirancang, pembahasannya hasil uji coba dari sistem 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 referensi perbaikan dimasa yang akan datang.