BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Setiap *Short Message Service* (SMS) yang masuk pada perangkat seseorang merupakan suatu privasi bagi dirinya. Sebagai contoh penyadapan SMS singkat yang pernah dialami oleh beberapa petinggi negara. Bagi dirinya penyadapan itu merugikan dirinya karena beberapa rahasia pribadinya terbongkar ke khalayak ramai. Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting, dalam hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Oleh karena itu, untuk menjaga kerahasian SMS diperlukan sebuah sistem keamanan yang berupa aplikasi keamanan dari suatu pesan.

Bahasa adalah kemampuan yang dimiliki manusia untuk berkomunikasi dengan manusia lainnya menggunakan tanda, misalnya kata dan gerakan. Bahasa Hakka secara harafiah berarti bahasa keluarga tamu atau di Indonesia umumnya dipanggil Khek adalah bahasa yang dituturkan oleh orang Hakka, yakni suku Han yang tersebar di kawasan pegunungan provinsi Guangdong, Fujian dan Guangxi di Tiongkok. Masing-masing daerah ini juga memiliki khas dialek Hakka yang agak berbeda tergantung provinsi dan juga bagian gunung sebelah mana mereka tinggal.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan atau informasi yang dapat dibaca. Pesan biasanya disebut juga sebagai *plaintext* [1]. Algortima *Advanced Encryption Standard* (AES) merupakan algoritma kriptografi modern yang bersifat simetris. Pada algoritma AES kunci yang dipakai memiliki panjang bervariasi yaitu 128,192,256 dengan memiliki jumlah ronde yang berbeda pula tergantung panjang kunci-nya, sehingga algoritma ini sangat baik untuk pengaman teks maupun data [1].

Pada awalnya *sender* mengisi pesan, kemudian pesan di terjemahkan ke bahasa khek dialek lufang, pesan hasil terjemahan kemudian dikirim dienkripsi dengan 16 kunci dan menghasilkan *Ciphertext*, saat mendekripsi pesan *recipient* menggunakan kode yang digunakan saat enkripsi, kemudian pesan diterjemahkan

kembali ke dalam bahasa indonesia. Maka dalam menjaga rahasia pesan yang dikirim, penulis mencoba membuat aplikasi enkripsi berbasis *mobile* menggunakan algoritma enkripsi AES dan konversi bahasa khek dengan mempelajari data penelitian sebelumnya, yang terdiri dari 10 penelitian, seperti Penelitian[2] Mengenai "Aplikasi Enkripsi Sms Pada Telpon Selular Berbasis J2me Dengan Metode Vignere Cipher", Penelitian[3] Mengenai "Aplikasi Data Keamanan Sms Menggunakan Metode Enkripsi Berbasis Android", Penelitian[4] Mengenai "Perancangan Aplikasi Enkripsi Sms Dengan Algoritma Blowfish Berbasis Android", Penelitian[5] mengenai "Aplikasi Enkripsi Sms Dengan Metode Rsa Pada Smartphone Berbasis Android", Penelitian[6] mengenai "Analisis Dan Perancangan Aplikasi Enkripsi Sms Dengan Kombinasi Metode Substitusi Dan Aes Berbasis Android Di Kalangan Mahasiswa Stmik "Amikom" Yogyakarta", Penelitian[7] mengenai "Enkripsi Sms (Short Message Service) Pada Telepon Selular Berbasis Android", Penelitian[8] mengenai "Implementasi Algoritma Enkripsi Aes Dan Vigenere Cipher Pada Aplikasi Sms Berbasis Android", Penelitian[9] mengenai "Implementasi Algoritma Rc6 Untuk Dekripsi Dan Enkripsi Sms Berbasis Android",dan Penelitian[10] mengenai "Aplikasi Kamus Aneka Bahasa Daerah Berbasis Smartphone Android", Penelitian[11] mengenai "Aplikasi "Ijawa" Kamus Indonesia Jawa Berbasis Android Mobile", sehingga pesan yang dikirim tidak memiliki arti apapun bagi siapapun termasuk operator.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang ada, rumusan masalah yang akan dibahas pada penelitian ini adalah:

1. Bagaimana membuat suatu aplikasi enkripsi SMS pada perangkat *mobile android*?
2. Bagaimana mengimplementasikan algoritma AES untuk enkripsi pesan dalam aplikasi SMS berbasis *android*?
3. Bagaimana mengimplementasikan konversi bahasa khek di dalam aplikasi SMS berbasis *android*?

1.3 Batasan Masalah

Batasan masalah yang dapat diambil dari latar belakang di atas adalah:

1. Penelitian ini hanya membahas teknik pengamanan pesan dengan Algoritma *Advanced Encryption Standard* (AES) sebagai pengaman kunci.
2. Karakter yang digunakan menggunakan tabel ASCII 255.
3. Pada algoritma AES menggunakan panjang kunci 128 bit.
4. Bahasa yang digunakan adalah bahasa pemrograman *Java* dan *Eclipse* sebagai IDE.
5. *Input* berupa pesan SMS.
6. Spesifikasi SMS (panjang 1 pesan SMS) disesuaikan dengan standar teknologi *Global System for Mobile Communication* (GSM).
7. Aplikasi menggunakan telepon seluler berbasis sistem operasi *android*.
8. Hanya membahas keamanan sms dan tidak membahas keamanan jaringan.
9. Menggunakan *Library Java*x.*crypto*.
10. Dua belah pihak pengguna harus sama-sama menggunakan aplikasi ini.
11. Tidak bisa menambah kata dikamus bahasa khek Indonesia.
12. Aplikasi cocok digunakan pada layar 5 *inch*.
13. Kunci harus mengandung 8 karakter.
14. Tidak membahas proses pengiriman pesan.
15. Hasil terjemahan bahasa Indonesia ke khek menghasilkan 1 spasi.
16. Versi *android* minimal *lolipop*.
17. Tidak *support dual* sim pada *smartphone*.
18. Tidak menterjemakan rangkaian kata yang membentuk kalimat.

1.4 Metodologi Penelitian

Rancang bangun aplikasi enkripsi SMS menggunakan algoritma AES (*Advanced Encryption Standard*) berbasis *android* menggunakan model *Waterfall* sebagai pengembangan perangkat lunak. Model *waterfall* adalah proses pembuatan aplikasi *android* secara struktur dan berurutan sehingga metode ini sangat cocok untuk pembuatan aplikasi berbasis *android*. Metode penelitian dalam perangkat lunak ini menggunakan Metode Berorientasi Objek, sedangkan alat bantu yang

digunakan dalam pengembangan aplikasi adalah *Unified Modelling Languange* (UML).

1.5 Tujuan dan Manfaat

1.5.1 Tujuan Penelitian

Dalam menerapkan aplikasi *short message service* (SMS) untuk merahasiakan pesan dengan konversi bahasa khek menggunakan algoritma *advanced encryption standard* (AES) pada perangkat berbasis android.

1.5.2 Manfaat Penelitian

Diharapkan penelitian ini bermanfaat untuk:

1. Menambah pengetahuan penulis dalam melakukan proses enkripsi dan dekripsi suatu pesan dengan menggunakan algoritma *Advanced Encryption Standard* (AES).
2. Menambah pengetahuan penulis dalam melakukan proses menerjemahkan bahasa indonesia ke bahasa khek maupun sebaliknya.
3. Penelitian ini diharapkan dapat bermanfaat untuk meningkatkan keamanan pesan singkat yang bersifat rahasia.
4. Sebagai bahan refrensi bagi peneliti lain yang ingin membahas topik yang terkait dengan penelitian ini.

1.6 Sistematika Penulisan

Agar dalam penulisan tugas akhir ini dapat lebih terarah, maka penulis berusaha sedapat mungkin menyusun secara sistematis sehingga diharapkan tahap-tahap pembahasan akan tampak jelas kaitannya antara bab yang satu dengan bab yang lainnya. Adapun isi dari masing-masing bab tersebut adalah sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini telah diuraikan tentang penjelasan umum dari permasalahan yang dibahas berkaitan dengan penyusunan skripsi ini yang meliputi latar belakang, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab landasan teori merupakan tinjauan pustaka, menguraikan teori-teori yang mendukung judul, dan mendasari pembahasan secara detail. Pada bab ini juga dituliskan tentang *tools/software* (komponen) yang digunakan untuk pembuatan aplikasi atau untuk keperluan penelitian. Pada bab ini, uraian teori yang digunakan adalah uraian pendukung sesuai dengan topik skripsi yang diambil.

BAB III METODOLOGI PENELITIAN

Bab metodologi penelitian ini terdiri dari 3 bagian utama yaitu model pengembangan perangkat lunak, metode pengembangan sistem, dan *tools* (alat bantu dalam analisis dan merancang sistem informasi).

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini menjelaskan tentang analisis masalah sistem yang berjalan, analisis hasil solusi, analisis kebutuhan sistem usulan, analisis sistem, dan perancangan sistem. Serta implementasi dan pengujian *system*.

BAB V PENUTUP

Dalam bab ini dapat diuraikan tentang kesimpulan dan saran mengenai skripsi ini. Kesimpulan adalah mengemukakan kembali masalah penelitian kemudian menyimpulkan bukti-bukti yang diperoleh dan akhirnya menarik kesimpulan apakah hasil yang didapat (dikerjakan), layak untuk digunakan (diimplementasikan). Saran merupakan manifestasi dari penulis untuk dilaksanakan.