BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi saat ini telah memberikan pengaruh yang sangat besar bagi teknologi informasi dan telekomnikasi khususnya telepon seluler. Telepon seluler menyediakan berbagai fitur, salah satunya adalah media SMS *(Short Message Service)*. SMS merupakan suatu layanan yang memungkinkan pengguna untuk saling berkomunikasi dengan mengirimkan pesan singkat dengan cepat dan biaya yang kecil. Setiap SMS yang masuk pada perangkat seseorang merupakan suatu kerahasiaan bagi dirinya. Sebagai contoh penyadapan SMS singkat yang pernah dialami oleh beberapa orang. Bagi dirinya penyadapan itu sangat merugikan karena beberapa rahasianya terbongkar ke khalayak umum.

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting. Hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Disaat seseorang mengirim pesan yang bersifat rahasia tetapi tidak adanya pengaman suatu pesan, pesan tersebut akan terlihat oleh layanan sms *gateway* atau SMS *center*. Oleh karena itu, untuk menjaga kerahasian SMS diperlukan sebuah sistem keamanan yang berupa aplikasi pengaman dari suatu pesan. Namun setelah pesan dienkripsi akan membentuk karakter dan simbol yang panjang maka dari itu dibutuhkan sebuah algoritma yang untuk kompresi pesan tersebut menjadi lebih singkat.

Advanced Encryption Standard (AES) merupakan algoritma kriptografi modern yang bersifat simetris. Pada algoritma AES mampu mendukung panjang kunci 128, 192 dan 256 dan memiliki jumlah ronde yang berbeda pula tergantung kunci yang dipakai[1]. Algoritma *Huffman* merupakan algoritma kompresi yang tertua. Algoritma ini merupakan jenis *lossless* data *compression* data, yang tidak menghilangkan satu *byte* pun dan disimpan sesuai aslinya[2]. Dengan menggunakan kriptografi algoritma AES dapat mencegah terjadinya penyadapan pesan dan menjaga kerahasiaan pesan. Serta dengan menggunakan kompresi

algoritma *huffman* membuat pesan yang telah di enkripsi tidak terlalu panjang. Dalam menjaga kerahasiaan pesan yang dikirim, maka penulis membuat aplikasi enkripsi berbasis *mobile android* menggunakan kriptografi algoritma AES dan kompresi algoritma *huffman* dengan judul "Penerapan Kriptografi Algoritma AES serta Kompresi Algoritma *Huffman* pada Aplikasi *Message*"

Penelitian sebelumnya, yang terdiri dari 10 penelitian, seperti penelitian[2] mengenai "Implementasi Kriptografi dan Kompresi SMS menggunakan Algoritma Algoritma RC6 dan Algoritma *Huffman* berbasis *Android* oleh Laurentinus pada tahun 2017", penelitian[3] mengenai "Implementasi Algoritma AES 256 bit dan Kompresi menggunakan Algoritma *Huffman* pada Aplikasi *Voice Recorder* oleh Selvia Rahmawati, Ichsan Taufik, dan Gitarja Sandi pada tahun 2017", penelitian[4] mengenai "Implementasi Kriptografi Algoritma AES serta Algortima Kompresi *Huffman* dengan menggunakan pemrograman PHP oleh Aris, Sanny Sahara, Nurul Aini, Mety Trisna Ajija dan Risa Nailil Mauna pada tahun 2017", penelitian[5] mengenai "Implementasi Kombinasi Algoritma Enkripsi AES 128 dan Algoritma Kompresi *Huffman* dengan menggunakan Pemrograman PHP oleh Heri Haryanto, Romi Wiryadinata dan Muhammad Afif pada tahun 2014", penelitian[6] mengenai "Pendekatan Keamanan serta Kecepatan Akses Data pada *Cloud* dengan Algoritma *Huffman* dan AES oleh Susanto Wahyu Eko pada tahun 2014", penelitian[7] mengenai "Implementasi Kriptografi menggunakan metode AES untuk Pengamanan Data Teks oleh Agustan Latif pada tahun 2015", penelitian[8] mengenai "Implementasi Teknik Kompresi Teks *Huffman* oleh Andysah Putera Utama Siahaan pada tahun 2016", penelitian[9] mengenai "Aplikasi Data Kemanan SMS menggunakan Metode Enkripsi berbasis *Android* oleh Dimas Mei Fajar pada tahun 2015", penelitian[10] mengenai "Penerapan Algoritma *Blowfish* untuk Keamanan SMS pada *Android* oleh Anton Prafanto pada tahun 2016", dan penelitian[11] mengenai "Aplikasi Enkripsi SMS dengan Metode RSA pada Smartphone berbasis *Android* oleh I Wayan Dharma Satriawan, I Gusti Made Arya Sasmita dan I Putu Agung Bayupati pada tahun 2014".

1.2 Rumusan 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 dan Kompresi *Huffman* untuk enkripsi pesan dalam aplikasi SMS berbasis *android*?

1.3 Batasan Masalah

Batasan masalah yang dapat diambil dari latar belakang diatas adalah:

1. Penelitian ini hanya membahas teknik pengamanan pesan dengan Algoritma *Advanced Encryption Standrad* (AES) sebagai pengaman kunci dan Algoritma *Huffman* sebagai kompresi teks.
2. Karakter yang digunakan menggunakan tabel ASCII 255.
3. Pada Algoritma AES menggunakan panjang kunci 128 bit.
4. Spesifikasi SMS (panjang 1 pesan SMS) disesuaikan dengan standar teknologi *Global System for Mobile Communication* (GSM).
5. Kunci harus menggunakan 8 karakter.
6. Versi *android* maksimal *lolipop*.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan

Untuk merahasiakan pesan menggunakan algoritma *Advanced Encryption Standard* (AES) serta kompersi algoritma *Huffman* pada aplikasi *Message*.

1.4.2 Manfaat

Diharapkan penelitian ini bermanfaat untuk: Mengamankan data pesan SMS selama proses pengiriman pesan dengan teknik kriptografi menggunakan algoritma *Advanced Encryption Standard* (AES) dan kompersi algoritma *Huffman*.

1.5 Sistematika Penulisan

Agar dalam penulisan tugas akhir ini dapat lebih terarah, maka penulis menyusun secara sistematis tahap - tahap pembahasan sehingga tampak jelas

kaitannya antara bab 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, 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 sistem.

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) dan saran merupakan manifestasi dari penulis untuk dilaksanakan.