BAB I
PENDAHULUAN

1.1 Latar Belakang

Telepon selular merupakan alat komunikasi yang sudah dipakai oleh sebagian besar penduduk di dunia. Pada awalnya pengiriman pesan digital mengunakan telepon seluler dilayani olehprovider telekomunikasi melalui *Short Messaging Service* (SMS) atau *Multimedia Messaging Service* (MMS). SMS melayani pengiriman pesan singkat berbasis teks, dan MMSpengiriman pesan berbasis multimedia. SMS dan MMS menggunakan nomor telepon selulersebagai alamat pengirim dan penerima pesan.

Namun dengan semakin berkembangnya teknologi telepon seluler yang berbasis *smartphone*, banyak para pengembang aplikasi maupun *vendor smartphone* mengembangkan aplikasi *Instant Messaging* (IM) sebagai layanan pengiriman pesan digital. IMmenjadi semakin populer karena dianggap memiliki banyak kelebihan seperti memungkinkan seseorang untuk melakukan percakapan *(chat)private* dengan orang lain secara *real time*.

Seiring dengan semakin banyak digunakannya layanan IM, maka kekhawatiran mengenai keamanan data atau pesan yang akan dikirim sangat tinggi, apalagi jika data tersebut sangat penting atau rahasia. Pada IM, teks pesan yang dikirim melalui pengirim pesan instan dapat di-*interception* dengan mudah jika tidak melalui proses enkripsi dalam perjalanannya. Oleh karena itu, suatu proses enkripsi diperlukan untuk mengamankan pesan teks yang dikirimkan. Sistem enkripsi dapat meningkatkan tingkat keamanan pesan. Hal ini dapat mengurangi bocornya informasi kepada pihak-pihak yang tidak berkepentingan.

Algoritma AES-128 adalah sistem kriptografi kunci simetris 128-bit. Alasan dipilihnya algoritma ini adalah karena algoritma ini tergolong algoritma *stream chipper*. Selain itu, algoritma ini bisa diimplementasikan secara efisien pada berbagai prosesor maupun hardware khusus. Sehingga jika

diimplementasikan pada perangkat *mobile* (*smartphone Android*) cukup efisien dalam komputasinya.

Oleh karena itu dengan memanfaatkan keunggulan dari algoritma AES-128 dan melihat masalah keamananan data pesan yang tengah dihadapi, maka dalam tugas akhir ini penulis akan membuat sebuah sistem enkripsi *prototype community messaging* berbasis *Android*.

1.2 Perumusan Masalah

Beberapa masalah yang akan timbul dalam tugas akhir ini antara lain:

a. Bagaimana merancang keamanan sistem enkripsi menggunakan algoritma AES-128 yang akan berjalan pada *Prototype Community Messenger* berbasis *Android*.
b. Bagaimana performansi kerja *Prototype Community Messenger* berbasis *Android* setelah diberikan keamanan sistem enkripsi.
c. Bagaimana menguji keamanan sistem enkripsi yang telah diimplementasikan.
d. Bagaimana menganalisis algoritma AES-128 terhadap waktu eksekusi *(running time)* fungsi pada *Prototype Community Messenger* berbasis *Android*.

1.3 Tujuan dan Manfaat

Berdasarkan rumusan masalah yang telah diuraikan, maka didapat tujuan dari tugas akhir antara lain :

a. Menjelaskan tentang perancangan keamanan sistem enkripsi menggunakan algoritma AES-128 yang akan berjalan pada *Prototype Community Messenger* berbasis *Android*.
b. Menjelaskan tentang performansi *Prototype Community Messenger* berbasis *Android* setelah diberikan keamanan sistem enkripsi.
c. Menjelaskan tentang hasil analisis algoritma AES-128 terhadap waktu eksekusi *(running time)* fungsi pada *Prototype Community Messenger* berbasis *Android*.

d. Menjelaskan tentang waktu yang dibutuhkan untuk menjalankan algoritma AES-128 pada *Prototype Community Messenger* berbasis *Android.*

1.4 Batasan Masalah

Untuk mempermudah dan membatasi cakupan pembahasan masalah pada tugas akhir ini maka diberikan batasan-batasan sebagai berikut:

a. Platform aplikasi mobile berbasis *Android*.
b. Hanya membahas keamanan aplikasi dan tidak membahas keamanan jaringan.
c. Server layanan data merupakan *Virtual Private Server* (VPS).
d. Tidak membahas kompresi data

1.5 Metodologi Penelitian

1. Studi Literatur

   Studi Literatur ini dimaksudkan untuk mempelajari konsep dan teori-teori yang dapat mendukung proses perancangan dan realisasi aplikasi ini dari berbagai sumber yang bermacam-macam seperti buku tentang kriptografi, internet, jurnalyang berhubungan dengan keamanan sistem.

2. Perancangan dan Realisasi

   Meliputi implementasi konsep dan teori-teori yang telah diperoleh dalam merancangsistem keamanan agar berjalan pada aplikasi.

3. Implementasi dan pembuatan sistem dan aplikasi

   Pada tahap ini dilakukan implementasi berdasarkan kebutuhan dan kesesuain pada tahap sebelumnya menggunakan *java* (dengan SDK android) dan *sqlLite* pada aplikasi *mobile*, *Hypertext Preprocessor* (php) sebagai layanan *server* dan *mysql* sebagai *database server*.

4. Pengujian

   Melakukan pengujian sistem keamanan sesuai dengan spesifikasi sistem keamanan yang diinginkan pada aplikasi.

5. Penyusunan laporan tugas akhir

   Pada tahap ini dilakukan penyusunan laporan yang berisi dasar teori, dokumentasi dari perangkat lunak, dan hasil-hasil yang diperoleh selama pengerjaan tugas akhir.

1.6 Sistematika Penulisan

Sistematika penulisan yang akan digunakan pada tugas akhir ini adalah sebagai berikut:

BAB 1 Pendahuluan

Berisi latar belakang permasalahan, tujuan penelitian, perumusan masalah, pembatasan masalah dan asumsi yang digunakan, serta metode penelitian yang dilakukan.

BAB 2 Landasan Teori

Bab ini berupa uraian konsep dan teori dasar secara umum yang mendukung dalam pemecahan masalah, baik yang berhubungan dengan sistem maupun aplikasi.

BAB 3 Perancangan dan Realisasi

Pada bab ini dibahas mengenai perancangan dan realisasi aplikasi serta sistem.

BAB 4 Implementasi dan Pengujian

Bab ini membahas mengenai implemtasi dan pengujian aplikasi pada *smarthphone* dan melakukan pengujian *alpha, beta*, waktu enkripsi dan dekripsi, serta keakuratan pengiriman data.

BAB 5 Kesimpulan dan Saran

Berisi kesimpulan yang dapat diambil dari tugas akhir ini beserta saran untuk pengembangan selanjutnya.