

BAB I

PENDAHULUAN

Pada bagian ini dikemukakan hal yang melatar belakangi pentingnya dilakukan penelitian, rumusan, dan batasan permasalahan yang dilakukan dalam penelitian, tujuan dan relevansi atau manfaat penelitian terhadap perkembangan solusi dari permasalahan yang diangkat, serta sistematika penulisan dalam laporan tugas akhir ini.

1.1 Latar Belakang

Pengiriman informasi melalui jaringan elektronik dalam permasalahan ini adalah *chatting* menggunakan media *server* memiliki kerentanan dalam keamanan data yang dikirimkan tersebut. Layanan tersebut diketahui memiliki beberapa kelemahan, yaitu kelemahan terhadap masalah keamanan sistem. Kelemahan itu dikarenakan data yang dikirim ke dalam *server* menggunakan koneksi dengan jaringan global sehingga lebih rentan terhadap serangan *hacker*.

Kelebihan aplikasi *chat* adalah pelayanan *realtime* sehingga tidak perlu menunggu beberapa lama untuk mendapatkan informasi, selain itu chat bisa dianggap lebih murah daripada sms karena sistem pembayarannya berdasarkan data yang keluar dari *handset* tersebut yang dimasukkan dalam paket internet.

Untuk menjamin keamanan dan kerahasiaan informasi, dilakukan proses enkripsi dan dekripsi terhadap informasi yang akan dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara mengkonversi informasi asli menjadi informasi sementara sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengkonversi informasi sementara menjadi informasi asli. Jadi informasi yang dikirimkan selama proses pengiriman adalah data informasi yang terenkripsi, sehingga informasi asli tidak dapat diketahui oleh pihak yang tidak berhak. Informasi asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia. Permasalahan utama dalam proses enkripsi dan dekripsi adalah penentuan algoritma yang tepat dan efisien yang digunakan dalam proses enkripsi dan dekripsi tersebut. Pada proses enkripsi dibutuhkan algoritma yang dapat mengenkripsi data secara aman dan pada proses dekripsi dibutuhkan algoritma yang dapat mendekripsi kembali data tersebut dengan tepat. Untuk keperluan tersebut, diperlukan suatu algoritma untuk menghasilkan kunci yang

sangat rahasia yang akan digunakan dalam proses enkripsi dan dekripsi tersebut. Salah satu standar algoritma yang umum digunakan untuk proses enkripsi dan dekripsi data adalah *Data Encryption Standard (DES)*.

Android memiliki sejumlah keunggulan dan ini yang membuat Android sangat diburu. Ada sejumlah keuntungan *Google Android* yang akan anda dapatkan disamping sebagai perangkat lunak *open source*. Beberapa keuntungan antara lain:

- a. Kemampuan bagi siapa saja untuk menyesuaikan *platform Google Android* akan membuka kesempatan membuat aplikasi untuk pemain kecil dan baru yang tidak memiliki kekuatan finansial untuk berinteraksi dengan *operator* nirkabel seperti *AT & T* dan *Orange*.
- b. Konsumen akan mendapatkan keuntungan dari memiliki berbagai aplikasi *mobile* sebagai pilihan lain sejak monopoli *mobile phone* yang dipecahkan oleh *Google Android*.
- c. Meskipun ini akan tergantung pada *operator*, seseorang dapat mengkustomisasi ponsel menggunakan *platform Google Android* tidak seperti sebelumnya, bahkan sampai ke layar.
- d. Fitur seperti rincian cuaca, membuka layar, *RSS feed* dan bahkan ikon pada layar pembukaan akan dapat disesuaikan.
- e. Selain itu, sebagai akibat dari banyak ponsel yang membawa *Android*, perusahaan akan datang dengan produk inovatif seperti layanan berdasarkan lokasi akan menyediakan pengguna dengan informasi yang mungkin dibutuhkan.
- f. Informasi ini dapat termasuk mengetahui lokasi dari sebuah toko terdekat atau pompa bensin. Selain itu fungsi hiburan akan menjadi lebih tinggi dengan *Android* untuk menawarkan game *online real time multi player*.

Kelebihan *Android mobile* yang banyak membuat ponsel ini sangat diinginkan. Kemampuan telepon untuk menyimpan sejumlah aplikasi adalah salah satu fitur yang membedakannya dari ponsel lain di pasaran. Secara keseluruhan, ponsel *Android* sangat cocok untuk menangani kegiatan sehari-hari .

1.2 Perumusan Masalah

Permasalahan yang hendak dipecahkan kali ini adalah, Bagaimana membuat aplikasi *chatting* yang menggunakan algoritma enkripsi *DES*?

1.3 Tujuan dan Manfaat

Tujuan akhir dari pengerjaan tugas akhir ini adalah:

1. Memberikan keamanan lebih pada layanan pengiriman data ke *server* sehingga tidak dapat dibaca dengan mudah oleh orang yang tidak berhak.
2. Mengimplementasikan algoritma enkripsi *DES* dalam aplikasi *Chatting* pada *handset Android*.

1.4 Batasan Masalah

Agar tugas akhir ini lebih fokus maka ditetapkan beberapa batasan masalah diantaranya:

1. Hanya membahas pengaplikasian algoritma *DES*.
2. Sistem operasi minimal *Android Froyo*
3. Aplikasi tidak bisa *running in background*.
4. Pesan yang dikirimkan hanya berupa teks

1.5 Metodologi Pengerjaan Tugas Akhir

Pengerjaan Tugas akhir ini menggunakan metodologi sebagai berikut :

1. Studi Pustaka
Proses pengumpulan data dan informasi dengan mempelajari materi-materi tentang algoritma enkripsi *DES*.
2. Perumusan Masalah
Pada tahap ini yang dikejakan adalah merumuskan masalah yang didapat, dan menentukan kebutuhan sistem yang tepat untuk mengatasinya.
3. Analisa dan Perancangan
Pada tahap ini proses analisa sistem dan mulai dilakukan perancangan design dari sistem yang akan digunakan.
4. Implementasi
Pada proses ini dilakukan pengimplementasian metode Enkripsi data *DES* untuk melakukan enkripsi pada pengiriman *data text* pada *server*.

5. Evaluasi

Pada tahapan ini adalah melakukan evaluasi terhadap sistem yang dibuat. Apa bila terjadi kekurangan maka akan dilakukan perbaikan.

6. Penulisan Laporan

Tahap ini merupakan tahap terakhir dari penyusunan tugas akhir. Pada tahap ini dilakukan penulisan laporan dari tugas akhir yang dikerjakan.

1.6 Sistematika Penulisan

Adapun sistematika pembahasan tugas akhir ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini terdiri dari : latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bagian ini dijelaskan mengenai hal-hal yang melandasi atau yang akan digunakan sebagai pedoman untuk menyelesaikan permasalahan yang terdapat dalam penelitian ini.

BAB III : METODOLOGI PENELITIAN

Berisi tentang perancangan strategi yang diusulkan mulai dari skenario, desain *environment*, strategi gerak serang dan metode yang digunakan.

BAB IV : IMPLEMENTASI SISTEM

Pada bab ini menjelaskan tentang implementasi program yang telah dikerjakan. Meliputi penjelasan tentang arsitektur sistem, desain sistem, desain interface, dan menguraikan tentang hasil uji coba serta analisis terhadap sistem.

BAB V : PENUTUP

Pada bab ini yang berisi kesimpulan dan saran yang dihasilkan dari sistem yang telah diujicobakan.