BAB I
PENDAHULUAN

I.1 Latar Belakang Masalah

Saat ini komunikasi suara telah menjadi hal yang penting dalam kehidupan sehari-hari, seperti komunikasi suara dengan telepon yang berbasis analog maupun telepon selular yang berbasis digital. Ilmu pengetahuan dan teknologi yang terus berkembang juga berperan dalam perkembangan komunikasi suara, salah satunya adalah komunikasi suara digital dengan pengiriman pesan suara melalui *instant messenger* seperti BBM, Catfiz, Whatsapp, Telegram, dan aplikasi serupa lainnya. Hal ini dapat dilakukan karena terdapatnya fitur share audio pada aplikasi-aplikasi *instant messenger* yang dapat dimanfaatkan oleh pengguna dalam mengirim pesan berupa file audio/suara.

Dalam penggunaan pengiriman suara melalui *instant messenger*, sebagai contoh pada BlackBerry Messenger (BBM), data dari ponsel pengirim dikirim ke jaringan operator, kemudian menuju internet, melalui firewall, lalu menuju ke server BlackBerry dan barulah sampai kepada ponsel penerima. Setiap data yang dikirim dari smartphone dienskripsi dengan semacam private key yang terdapat di mailbox user. Dan data tersebut tetap tidak dapat dibaca saat dalam proses pengiriman. Kemudian, informasi yang masih terenskripsi tersebut bisa dibaca oleh smartphone penerima dengan teknologi pembaca enskripsi yang ada di dalamnya. Sehingga data yang terkirim diklaim aman oleh BlackBerry. (Detik Inet 2013, hlm.1)

Karena file yang dikirimkan disimpan pada server terlebih dahulu sebelum sampai ke penerima, maka terjadi ancaman dan kerentanan terhadap informasi dari isi file pesan suara. Walaupun semua pengembang aplikasi *instant messenger* mengklaim aplikasi buatannya aman, hal itu tidak serta merta dapat menjamin kerahasiaan dari isi pesan suara karena algoritma untuk melakukan enkripsi dibuat oleh penyedia layanan *instant messenger*, maka penyedia layanan pun dapat mengetahui dan membuka file pesan suara yang ada pada server.

Untuk mengatasi ancaman tersebut sehingga mengurangi resiko bahwa pesan suara yang dikirimkan dapat dibuka oleh pihak server, maka dilakukan proses enkripsi. Melalui cara ini akan dilakukan enkripsi terhadap pesan suara yang akan dikirimkan, maka meskipun ada pihak yang berhasil mengakses maupun mendapatkan data suara tersebut, pihak yang tidak dikehendaki tidak dapat memahami data suara yang dikirimkan karena data suara telah dienkripsi menjadi tidak bermakna serta perlu aplikasi yang dapat memutar data suara dan memasukkan kunci yang benar agar mendapat informasi asli dari pesan suara yang belum dienkripsi.

Pada skripsi ini akan digunakan dan dibahas algoritma RC6 karena algoritma kriptografi RC6 adalah algoritma yang sangat kuat. Algoritma ini memiliki performansi yang sangat baik walaupun besar cipherteks selalu sedikit lebih besar daripada besar plainteks, memiliki *avelache effect* yang kecil, dan tidak memiliki kunci lemah ataupun kunci setengah lemah. Sampai dengan saat ini, belum ada serangan yang secara signifikan dapat memecahkan kunci dari algoritma RC6 standar dalam tempo waktu yang singkat. (Rudianto n.d, hlm.6)

I.2 Perumusan Masalah

Berdasarkan latar belakang tersebut maka didapatkan rumusan masalah yaitu:

a. Bagaimana menjaga keamanan isi pesan suara agar tidak diketahui oleh pihak-pihak yang tidak dikehendaki?
b. Bagaimana membuat sebuah aplikasi yang dapat mengamankan pesan suara sebelum dikirimkan dan kemudian dilakukan pengiriman melalui *instant messenger*?
c. Bagaimana mengimplementasikan algoritma RC6 untuk melakukan enkripsi dan dekripsi pesan suara di *smartphone* berbasis android?

I.3 Batasan Masalah

Adapun batasan masalah dalam penulisan tugas akhir ini adalah:

a. Penelitian ini difokuskan pada penggunaan algoritma *Rivest Code* 6 (RC6) dan tidak mebahas perhitungan manual *Rivest Code* 6 (RC6) terhadap enkripsi file suara.
b. Perancangan program enkripsi dekripsi pesan suara ini menggunakan bahasa Java dan xml diimplementasikan kebentuk Apk lalu di*install* pada *smartphone* android yang digunakan.
c. Aplikasi yang dibangun akan terpisah dengan *instant messenger*.
d. Aplikasi *instant messenger* yang dapat digunakan untuk melakukan pengiriman file pesan suara terenkripsi (*chipertext*) hanya yang mempunyai fitur *share* file seperti BBM, telegram.
e. Aplikasi yang dikembangkan hanya dapat digunakan di sistem android API 14 (Ice Cream Sandwich) keatas.
f. Kedua belah pihak yang melakukan proses komunikasi pesan suara ini harus menggunakan aplikasi yang dibuat untuk dapat melakukan proses enkripsi serta dapat memainkan pesan suara yang diterima dengan cara melakukan dekripsi terlebih dahulu.

I.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

a. Membuat aplikasi yang dapat merekam suara, kemudian dilakukan enkripsi terhadap pesan suara yang direkam agar dapat meningkatkan kemanan pesan suara dan kemudian dikirim melalui *instant messenger*.
b. Mengimplementasikan algoritma RC6 untuk pengamanan pesan suara.

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dalam penelitian ini sebagai berikut:

a. Bagi IPTEK, Menambah pengetahuan tentang algoritma *Rivest Code 6* (RC6) dan penggunaannya untuk mengenkripsi pesan suara.

b. Bagi pengguna, dapat melakukan pengiriman pesan suara dengan *instant messenger* secara aman karena pesan suara telah dienkripsi sehingga dibuat tidak bermakna dan tidak dapat dimainkan.

I.6 Luaran yang Diharapkan

Sebuah aplikasi yang dapat melakukan perekaman suara yang kemudian dienkripsi menggunakan algoritma RC6 dan kemudian dikirim melalui *instant messenger*.

I.7 Sistematika Penulisan

Dalam penyusunan skripsi ini penulis menyajikan sistem penulisan sejelas mungkin tanpa keluar dari pokok permasalahan, sehingga pembaca dapat memahami setiap bagian dalam pembahasannya. Dibawah ini merupakan sistematis skripsi yang terbagi kedalam beberapan bab dan disusun sebagai berikut.

BAB I PENDAHULUAN

Bab ini menjelaskan tentang gambaran umum penulisan yang terdiri dari Latar Belakang, Perumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Luaran yang Diharapkan, dan Sistematika Penulisan.

BAB II LANDASAN TEORI

Dalam bab ini penulis menjelaskan konsep dasar sebagai bahan rujukan yang dibahas berdasarkan pembatasan masalah penulisan ini, dan juga memberikan penjelasan teori-teori yang relevan untuk menunjang penulisan tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang langkah-langkah penelitian yang digunakan agar tercapai luaran yang diharapkan sehingga tujuan dan manfaat penelitian benar-benar terpenuhi.

BAB IV ANALISA DAN IMPLEMENTASI

Bab ini akan membahas tentang analisa kebutuhan sistem, perancangan sistem, implementasi dari perancangan yang telah dilakukan kedalam program aplikasi, serta pengujian dan hasil.

BAB V PENUTUP

Bab ini penulis menyampaikan kesimpulan dan saran dari hasil penelitian yang telah dilaksanakan dan disusun pada bab sebelumnya.

DAFTAR PUSTAKA

Pada halaman ini berisi daftar referensi yang digunakan dalam penyusunan proposal skripsi, referensi dari internet, buku dan lain lain.

RIWAYAT HIDUP