BAB I
PENDAHULUAN

1.1. Latar Belakang

Instant Messaging (IM) adalah salah satu perangkat *computer-mediated communication* (CMC) (Lancaster et al., 2007) yang dikenal sebagai aplikasi bebas yang memungkinkan pengguna untuk tukar menukar pesan secara instan. Kemampuan *Instant Messaging* dalam menyediakan cara berkomunikasi yang mudah dan menyenangkan yang membuat *Instant Messaging* saat ini menjadi populer. *Instant Messaging* telah menjadi standar aplikasi pesan berbasis Internet yang saat ini menggantikan *e-mail* (Lancaster et al., 2007).

Tingkat keamanan tentunya menjadi salah satu aspek penting dalam pengiriman informasi melalui *Instant Messaging* (Symantec Enterprise Security, 2002), untuk menghindari terjadinya pencurian informasi pada pesan oleh pihak ketiga yang akan berakibat pada keamanan pesan yang dipertukarkan. Hingga saat ini kelemahan tersebut masih belum begitu disadari oleh pengguna yang memiliki informasi rahasia saat berkomunikasi lewat *Instant Messaging* (Nugraha, 2010). Untuk itu dibutuhkan aplikasi yang mampu melindungi kerahasiaan pesan dari pihak ketiga yang mencoba menyadap dan mencuri informasi pada *Instant Messaging*. Solusi dari permasalahan tersebut adalah dengan cara proses enkripsi pesan yang akan dikirimkan.

Salah satu algoritma kriptografi yang dapat digunakan untuk mengamankan pesan atau informasi adalah algoritma *Key Dependent Secure Messenger* yang menghasilkan tingkat *avalanche effect* yang tinggi, panjang kunci yang lebih tinggi akan memberikan keamanan yang lebih tinggi tetapi dapat meningkatkan waktu eksekusi algoritma *key* (suatu barisan yang digunakan sebagai kunci) untuk mendapatkan *pseudorandom key* yang akan diinisialisasikan dengan 2 (dua) tahapan untuk mengenkripsi pesan dengan mengambil 128 bit *plaintext*, membagi *plaintext* menjadi dua bagian, membalikkan setiap bagian, kemudian menukar keduanya.

Setelah dilakukan tahapan algoritma untuk mengenkripsi pesan akan berpengaruh pada pembentukan *key* (kunci) dan tentunya akan menghasilkan perubahan *ciphertext* yang signifikan pada *plaintext* yang sama sehingga bisa memenuhi persyaratan *avalanche effect* pada saat pengujian *ciphertext*. Setiap kali melakukan pengiriman pesan maka *key* (kunci) yang digunakan akan selalu berbeda, jika pihak ketiga mendapatkan *key* (kunci) tersebut tentu tidak akan bisa digunakan dalam proses dekripsi selanjutnya sehingga pada proses pengiriman, pesan asli tidak dapat dibaca terhadap penyadapan.

Berdasarkan uraian di atas dapat disimpulkan untuk mengangkat topik tugas akhir dengan judul **"Implementasi Algoritma Key Dependent Secure Messenger Pada Instant Messaging"**.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang diatas, maka yang menjadi rumusan masalah adalah perlunya melakukan penerapan *Key Dependent Secure Messenger* pada *Instant Messaging* dengan membangkitkan *key* (kunci), sehingga pihak ketiga tidak akan mudah mengetahui *key* (kunci) yang digunakan pada enkripsi dan dekripsi.

1.3. Tujuan dan Manfaat

Adapun tujuan dari penelitian ini adalah menghasilkan aplikasi *instant messaging* dengan menggunakan *Key Dependent Secure Mesenger* yang akan menghasilkan *key* (kunci) untuk diimplementasikan kedalam algoritma *Key Dependent Secure Mesenger.*

Adapun manfaat yang diharapkan dari penelitian yang dilakukan adalah aplikasi yang dibuat dapat digunakan untuk menjaga kerahasiaan atau keamanan pesan, sehingga pengirim pesan merasa aman terhadap pesan yang dikirim maupun yang diterima tanpa diketahui pihak lain.

1.4. Batasan Masalah

Adapun batasan masalah dalam pelaksanaan tugas akhir ini antar lain.

1. Algoritma hanya bekerja pada 128 bit
2. Algoritma hanya menggunakan 1 kunci pada setiap proses pengiriman pesan.
3. Aplikasi terbatas hanya pada pengolahan teks.
4. Panjang pesan 160 karakter.
5. Karakter yang dikirimkan hanya bisa bernilai ASCII antara 0 sampai 255.
6. Aplikasi berbasis *client – server,* menggunakan laptop dan dua *client* menggunakan aplikasi *smartphone* (berbasis android).
7. Antarmuka *user* dengan sistem menggunakan aplikasi *smartphone*.
8. Tidak mendukung operasi *file transfer.*
9. Tidak mendukung input berupa *audio* dan *video.*
10. Topologi jaringan dirancang pada jaringan *local area network* (LAN).

1.5. Metodologi Penelitian

Langkah - langkah yang ditempuh dalam pengerjaan tugas akhir ini adalah sebagai berikut :

1. Studi Literatur

   Pada tahapan ini adalah tahap untuk mencari referensi untuk tugas akhir dari berbagai buku, jurnal, situs, dan paper sebagai sumber untuk landasan teori serta mempelajari referensi dari sumber yang telah didapat. Berdasarkan dari sumber yang telah didapatkan, tahapan yang harus dipelajari pada tugas akhir ini adalah sebagai berikut :

   a. Proses pembentukan kunci (*key*) dilakukan dengan menggunakan fungsi *random* yang terdiri dari 16 karakter..
   b. Proses enkripsi dan dekripsi pada metode kriptografi dengan menggunakan algoritma *key dependent secure messenger*.

2. Pengembangan Aplikasi

Pada tahap ini pengembangan aplikasi akan menggunakan tahapan dari metode waterfall. Metode waterfall adalah suatu proses pengembangan perangkat lunak secara terstruktur dan berurutan dimulai dari Analisis Kebutuhan, Desain Sistem, Pengujian Kode Program, yaitu

a. Analisis kebutuhan

Proses analisis ini mencakup analisis proses dan pemodelan sistem. Persyaratan fungsional dan non-fungsional dari sistem yang akan dirancang, dimana analisis fungsional akan menggunakan *use case.*

b. Desain sistem

Pada tahapan ini, terdapat proses perancangan dari aplikasi yang akan dibangun, seperti perancangan *User Interface*, perancangan pada pemodelan sistem, dan sebagainya. Berikut adalah rancangan antarmuka (*interface*) dari aplikasi yang akan dibuat:

i. Rancangan antarmuka *login.*
ii. Rancangan antarmuka *register*.
iii. Rancangan antarmuka *chats*.
iv. Rancangan antarmuka *udpate.*
v. Rancangan antarmuka *contacts.*
vi. Rancangan antarmuka *settings..*
vii. Rancangan antarmuka *invite.*
viii. Rancangan antarmuka *dashboard* pada halaman *admin.*
ix. Rancangan antarmuka *avalanche effect test* pada halaman *admin.*
x. Rancangan antarmuka *menage users* pada halaman *admin.*
xi. Rancangan antarmuka *edit profile* pada halaman *admin.*

c. Penulisan kode program

Pada tahap implementasi, dilakukan pengkodean dan perancangan aplikasi yang telah dibuat sebelumnya kedalam bahasa pemrograman. Bahasa pemrograman yang digunakan adalah PHP, JQuery, CodeIgniter v2.2.0, AJAX dimana proses pengetikan kode program (*coding*) dilakukan pada aplikasi Aptana Studio v3.6.0 beta. Penyimpanan data *user* dan data pesan

disimpan pada database dengan menggunakan aplikasi Xampp v3.1.0 beta.

3. Pengujian

   Tahapan ini merupakan proses akhir dimana sistem yang baru akan diuji yaitu:

   a. Pengujian yang dilakukan dengan menggunakan *avalanche effect* untuk mengetahui baik atau tidaknya algoritma yang digunakan. Pengujian ini dilakukan dengan membandingkan *ciphertext* yang dihasilkan dengan perbedaan 1 bit pada *plaintext* maupun kunci yang digunakan. Jika hasil menunjukkan terjadi perubahan bit berkisar antara 40% - 60%, maka algoritma kriptografi yang digunakan dikatakan baik karena akan menghasilkan *ciphertext* yang sangat acak sehingga menyulitkan bagi kriptanalis.

   b. Pengujian yang dilakukan dengan menangkap pesan atau paket data yang melintas dalam suatu jaringan dengan menggunakan aplikasi *WireShark,* dan membuktikan bahwa pesan yang dikirim merupakan *chipertext* yang akan dihasilkan oleh *Key Dependent Secure Messenger.*

4. Penarikan Kesimpulan

   Pada tahap ini penarikan kesimpulan diambil berdasarkan hasil pengujian yang dilakukan pada tahapan sebelumnya.

5. Menyusun Laporan Tugas Akhir