1. Pendahuluan

1. Latar Belakang

Masalah keamanan pada pesan merupakan salah satu masalah yang terdapat dalam sebuah komunikasi yang berlangsung melalui internet. Banyak media yang digunakan sebagai sarana untuk berkomunikasi, salah satunya adalah *instant messaging. Instant messaging* menjadi pilihan bagi sebagian besar masyarakat dunia untuk melakukan komunikasi. Hai ini dikarenakan layanan *instant messaging* memiliki beberapa kelebihan dibandingkan dengan layanan komunikasi lainnya. Salah satu contoh dari layanan komunikasi yang memiliki *Instant messaging* adalah *Yahoo*!. Pengiriman pesan pada protocol YMSG yang digunakan oleh *Yahoo*! Messenger dilakukan dengan melakukan transaksi paket antar *client* dan *server*. Sayangnya, pesan yang dienkapsulasi ke dalam paket – paket tersebut tidak mengalami proses enkripsi, sehingga pesan yang dikirim dapat dengan mudah dibaca oleh penyusup/*hacker*. Untuk meningkatkan keamanan, maka perlu diimplementasikan suatu sistem enkripsi pada *client* sebelum dikirim ke *server*.

Kandidat algoritma yang digunakan untuk melakukan proses enkripsi pengiriman pesan pada aplikasi Instant Messaging adalah *blowfish*, *twofish*, dan *AES* (Rijndael). Dimana *blowfish* menggunakan blok berukuran 64 bit, cepat, menggunakan operasi – operasi sederhana dan panjang kunci mulai dari 64 bit hingga 448 bit. Sedangkan *twofish* menggunakan blok berukuran 128 bit dan panjang kunci 128, 192, atau 256 bit merupakan finalis dari lomba untuk menetapkan standar *AES*. Begitu juga dengan *Rijndael*, yang mendapat gelar sebagai algoritma enkripsi terbaik menggunakan blok berukuran 128 bit dengan panjang kunci 128, 192, atau 256 bit.

Penggunaan metode enkripsi *twofish* pada aplikasi *Instant Messaging* akan lebih efektif dibandingkan dengan algoritma *blowfish* dan *AES* pada panjang kunci 256 bit, sedangkan pada penggunaan kunci dengan panjang 128 bit *AES* lebih unggul dengan perbedaan waktu yang tidak terlalu signifikan. Keamanan yang diberikan oleh ketiga algoritma tersebut cukup baik, perlu waktu bertahun – tahun untuk dapat melakukan cracking terhadap algoritma tersebut.

Untuk menanggulangi permasalahan tersebut, dalam Tugas Akhir ini akan diimplementasikan sebuah sistem *Secure Instant Messaging* menggunakan bahasa pemrograman Java dengan metode *Blowfish, Twofish*, dan *AES* yang bertujuan untuk melakukan enkripsi terhadap pesan yang akan dikirim dengan menggunakan protokol YMSG, agar aplikasi dapat terhubung langsung dengan server *Yahoo*! *Messenger*. Setelah itu akan dilakukan analisa terhadap sistem dengan cara melakukan penyadapan menggunakan *tools abel&chain* dan *wireshark* untuk melakukan pengujian apakah pesan yang dikirim sudah terenkripsi dengan baik atau belum.

1.2 Perumusan Masalah

Permasalahan yang dihadapi dalam pengimplementasian *instant messaging* Menggunakan Metode Kriptografi *Blowfish, Twofish, dan AES* ini adalah :

1. Bagaimana cara untuk membuat aplikasi *Instant Messaging* dengan menggunakan bahasa pemrograman Java dan protokol YMSG.
2. Bagaimana cara mengimplementasikan algoritma *Blowfish, Twofish,* dan *AES* pada aplikasi *Instant Messaging* agar pesan yang dikirim dapat terenkripsi.
3. Bagaimana cara untuk mengukur waktu yang dihasilkan oleh ketiga algoritma tersebut.
4. Bagaimana cara untuk menguji keamanan sistem enkripsi yang telah diaplikasikan pada perangkat lunak.

1.3 Tujuan

Adapun tujuan dari pengerjaan Tugas Akhir ini adalah :

1. Membangun aplikasi *instant messaging* yang aman (*secure*) menggunakan metode enkripsi *Blowfish, Twofish, dan AES* dengan bahasa pemrograman Java dan protocol YMSG.
2. Membuat aplikasi tersebut dapat terhubung dengan server Yahoo!, dan dapat melakukan komunikasi (chatting) dengan *client* lainnya menggunakan koneksi internet.
3. Menjamin kerahasiaan pesan dengan cara melakukan enkripsi terhadap pesan sebelum pesan dikirim, dan dekripsi setelah pesan diterima.
4. Mempersingkat sistem keamanan pada sistem dengan cara melakukan proses pembangkit kunci, kemudian disimpan kedalam sebuah variabel. Sehingga sistem tidak perlu melakukan proses pembangkit kunci saat ingin melakukan enkripsi – dekripsi, kecuali kunci mengalami perubahan.
5. Melakukan analisa terhadap aplikasi dengan cara melakukan penyadapan menggunakan tools *abel&chain* untuk melakukan sniffing pada pada komputer target dan *wireshark* untuk melakukan pengujian apakah pesan yang dikirim sudah terenkripsi dengan baik atau belum.
6. Menentukan metode enkripsi yang paling tepat untuk diimplementasikan pada *instant messaging.*

1.4 Batasan Masalah

Batasan masalah untuk proposal Tugas Akhir ini adalah :

1. Implementasi aplikasi *instant messaging* ini menggunakan bahasa pemrogramman Java.
2. Implementasi aplikasi ini menggunakan sistem operasi windows XP SP3. Karena tools yang digunakan untuk membangun sistem berjalan dengan baik pada sistem operasi windows XP SP3.
3. Analisa pengujian dilakukan dengan cara melakukan *sniffing* menggunakan tools *abel&chain* dan *wireshark.* Karena tools tersebut berjalan cukup baik untuk melakukan penyadapan terhadap data yang mengalir pada jaringan
4. Aplikasi ini tidak menggunakan metode pertukaran kunci, diasumsikan *user* sudah melakukan pertukaran kunci dengan aman.
5. Dalam tugas akhir ini metode yang dibahas hanyalah *Blowfish, Twofish, dan AES*, tidak membahas algoritma lain yang digunakan untuk melakukan perbandingan.
6. Aplikasi ini hanya melakukan enkripsi, dekripsi, dan pengiriman data dalam bentuk text.
7. Pengukuran waktu hanya dilakukan terhadap waktu tambahan mekanisme keamanan, diluar waktu pengiriman data melalui media internet.

1.5 Metode Penelitian

Metode penelitian yang digunakan untuk implementasi Tugas Akhir ini adalah :

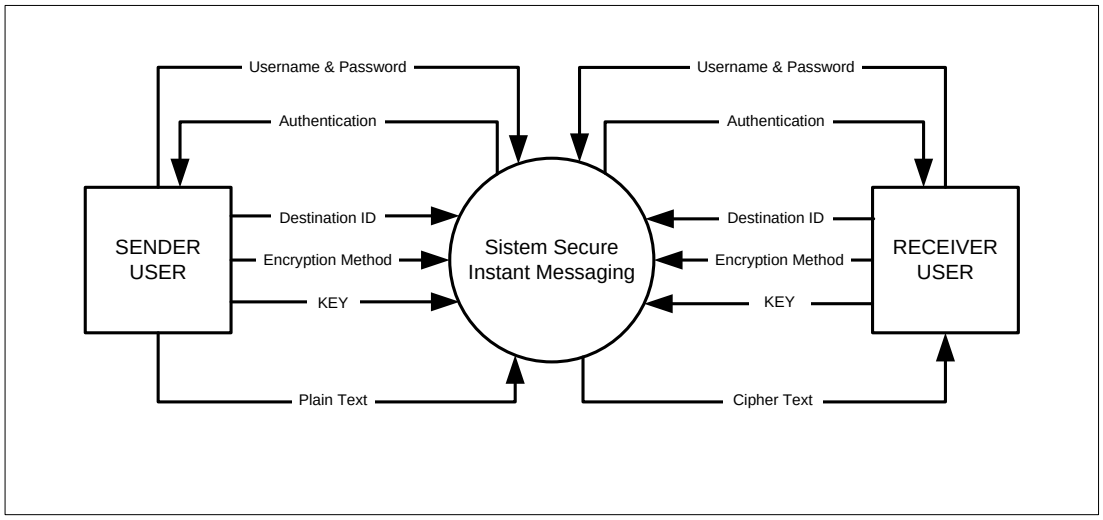
1. Studi literature

Dalam tahap ini akan dilakukan pencarian sumber yang dapat menjadi acuan dalam pengerjaan Tugas Akhir ini dan pemahaman materi tentang algoritma kriptografi yang digunakan dalam sistem *Secure Instant Messaging*.

2. Perancangan model dan implementasi

Melakukan perancangan terhadap aplikasi yang akan dibangun, kemudian melakukan implementasi berdasarkan rancangan tersebut.

Berikut adalah contoh *context diagram* dari perancangan sistem *Secure Instant Messaging* :



Gambar 1-1: *Context Diagram* Pada *Secure Chatting*

3. Pengujian dan analisa hasil implementasi

Pengujian terhadap aplikasi ini dilakukan dengan cara membandingkan waktu dan keamanan yang dihasilkan oleh metode *blowfish*, *twofish*, dan *AES*. Pengukuran waktu dilakukan melalui tiga tahap, yaitu pengukuran waktu pada saat melakukan proses pembangkit kunci, pengukuran waktu pada saat melakukan enkripsi, dan pengukuran waktu pada saat melakukan dekripsi.

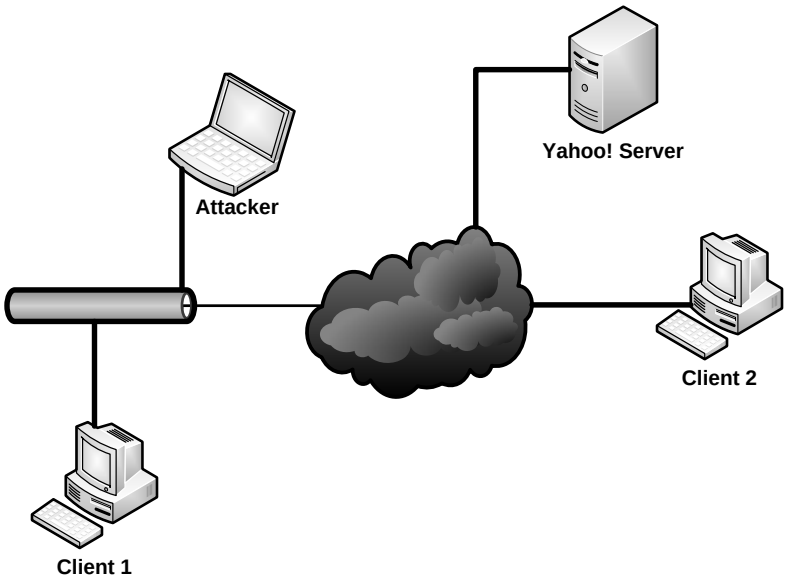
Pengujian waktu proses terhadap ketiga algoritma tersebut menggunakan beberapa variabel, diantaranya :

- Besar ukuran kunci yang digunakan (128 bit, 192 bit, dan 256 bit).
- Besar ukuran pesan, dibagi menjadi 3 kategori, yaitu untuk pesan berukuran pendek menggunakan 50 karakter, pesan berukuran sedang menggunakan 200 karakter, dan pesan berukuran panjang menggunakan 400 karakter.

Sedangkan untuk pengujian keamanan dilakukan dengan cara melakukan penyadapan pesan terhadap *user* yang sedang berkomunikasi untuk melihat apakah pesan yang dikirim sudah terenkripsi atau belum. Kemudian untuk mengukur tingkat kesulitan seorang *attacker* untuk melakukan *cracking*, digunakan rumus matematis untuk dapat memperkirakan waktu yang dibutuhkan untuk meng-*crack* algoritma tersebut.

Analisa hasil implementasi dilakukan dengan cara mengambil data waktu proses dari ketiga algoritma yang digunakan (berdasarkan variabel) sebanyak 30 kali, kemudian

dihitung rata – ratanya, sehingga dapat disimpulkan waktu total yang dihasilkan oleh masing – masing algoritma.



Gambar 1-2: Skenario Pengujian

1.6 Jadwal Kegiatan

Jadwal kegiatan pengerjaan Tugas Akhir adalah sebagai berikut :

Tabel 1-1: Tabel jadwal kegiatan

Kegiatan	**Bulan ke-1**	**Bulan ke-2**	**Bulan ke-3**	**Bulan ke-4**	**Bulan Ke-5**	**Bulan Ke-6**	**Bulan Ke-7**
Pengumpulan data							
Pembangunan model							
Implementasi							
Analisa hasil							
Pembuatan laporan							