SECURE CHATTING (INSTANT MESSAGING) MENGGUNAKAN METODE ENKRIPSI BLOWFISH, TWOFISH, DAN AES

Angga Kusumah[1], Maman Abdurrohman[2], Dodi Wisaksono Sudiharto[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Aplikasi pengiriman pesan instant (Instant Messaging) sudah menjadi hal yang umum digunakan oleh masyarakat luas. Kemampuan pengiriman pesan secara cepat membuat user dapat berkomunikasi satu sama lainnya secara real-time. Salah satu aplikasi Instant Messaging yang umum digunakan adalah Yahoo! Messenger. Aplikasi ini melakukan enkapsulasi terhadap pesan berupa plainteks (tidak menggunakan metode enkripsi), sesuai dengan protokol yang diberikan oleh Yahoo!. Oleh karena itu seorang attacker dapat membaca pesan yang dikirim dengan mudah. Agar user dapat menggunakan aplikasi instant messaging dengan aman, maka diimplementasikan sebuah sistem Secure Instant Messaging.

Aplikasi Instant Messaging ini dibangun menggunakan API jYMSG menggunakan bahasa pemrograman Java. Pada API jYMSG sudah disediakan protokol – protokol yang digunakan oleh Yahoo! sehingga pesan ter-enkapsulasi sesuai dengan protokol yang digunakan oleh Yahoo!.

Algoritma enkripsi yang digunakan pada sistem keamanan ini adalah Blowfish, Twofish, dan AES. hal tersebut disesuaikan dengan standar kecepatan proses dan keamanan dari ketiga metode tersebut. Pengaplikasian metode enkripsi pada aplikasi Instant Messaging cukup penting untuk memberikan keamanan dari serangan attacker. Sistem keamanan ini melakukan enkripsi terhadap pesan sebelum pesan dikirim oleh sender ke server Yahoo!, dan melakukan dekripsi saat sampai pada receiver sebelum pesan ditampilkan. Sehingga pesan sudah berupa cipherteks saat ditransmisikan melalui media tertentu. Pengukuran dilakukan terhadap waktu proses dan perkiraan tingkat keamanan yang diberikan oleh ketiga algoritma tersebut.

Kata Kunci : Instant Messaging, Yahoo!, jYMSG, Algoritma enkripsi, Blowfish, Twofish, AES, sistem Secure Instant Messaging.

Abstract

Instant messaging applications has become commonly used by the public. Instant messaging capability allows the user to communicate with each other in real-time. One of the Instant Messaging application that is commonly used Yahoo! Messenger. These applications perform encapsulation of a plaintext message, according to the protocol provided by Yahoo!. Therefore, an attacker can read the messages sent with ease. So that users can use instant messaging applications with a secure, then implemented a Secure Instant Messaging system.

Instant Messaging applications are built using the API jYMSG using the Java programming language. In jYMSG API already provided protocols used by Yahoo!, so the message was encapsulated in accordance with the protocol used by Yahoo!.

Encryption algorithm used in this security system is Blowfish, Twofish, and AES. It is adjusted to the speed of the process and security standards of all three methods. Application of the method of encryption on the Instant Messaging application is important enough to provide security from attack attacker. This security system encrypts the message before the message sent by the sender to the Yahoo! servers, and perform decryption time until the receiver before the message is displayed. So the message is in the form of ciphertext when transmitted over certain media. Measurements carried out on processing time and the estimated level of security provided by the third algorithm.

Keywords : Instant Messaging, Yahoo!, jYMSG, Encryption algorithm, Blowfish, Twofish, AES, Secure Instant Messaging system.

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.

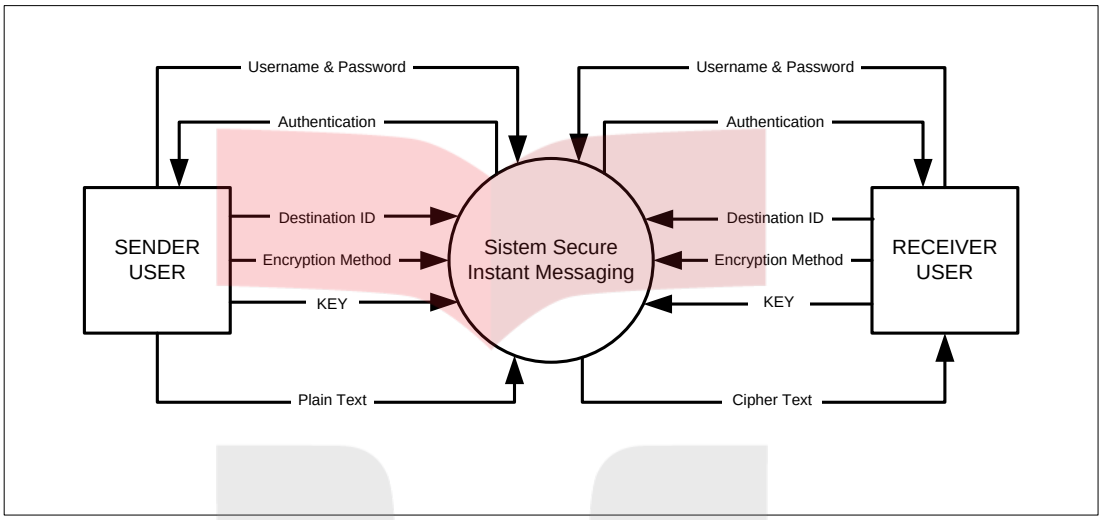
1.5 Metode Penelitian

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.

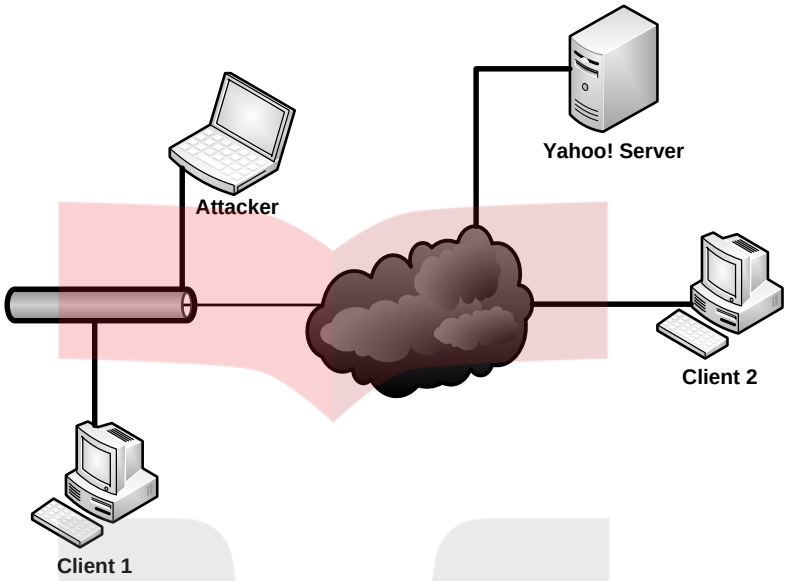
Pengujian waktu proses terhadap ketiga algoritma tersebut menggunakan beberapa variabel, diantaranya :

- 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							

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan pengujian yang telah dilakukan terhadap sistem *Secure Instant Messaging* menggunakan algoritma *Blowfish, Twofish,* dan *AES,* dapat diambil kesimpulan sebagai berikut :

1. Dari ketiga algoritma yang diuji, algoritma AES memberikan performasi yang paling baik, mulai dari perbandingan waktu proses pembangkit kunci dan proses enkripsi – dekripsi. terutama pada penggunaan pesan pendek (50 karakter) dan sedang (200 karakter). Sedangkan pada penggunaan pesan panjang (400 karakter) perbedaan waktu antara ketiga algoritma tidak terlalu signifikan. Tetapi Algoritma *AES* masih unggul pada penggunaan kunci sebesar 128 bit dan 256 bit. Sehingga dapat disimpulkan bahwa algoritma *AES* merupakan algoritma yang pas untuk sistem *Secure Instant Messaging* dilihat dari segi tambahan waktu proses (diluar waktu pengiriman pesan melalui media internet).
2. Dari ketiga algoritma yang diuji, keamanan yang diberikan relatif sama. Setiap algoritma melakukan proses enkripsi dan dekripsi dengan baik. Sehingga pada saat pesan dikirimkan, *attacker* tidak dapat membaca isi dari pesan tersebut. Dan satu – satunya metode *cracking* yang dapat digunakan terhadap sistem adalah *brute-force attack.* Untuk dapat melakukan *cracking* dengan metode *brute-force attack* membutuhkan waktu bertahun – tahun. Sehingga dapat disimpulkan bahwa pengiriman pesan yang dilakukan oleh sistem *Secure Instant Messaging* aman.

5.2 Saran

Saran – saran yang diberikan terkait dengan tugas akhir ini adalah :

1. Perangkat lunak yang dibangun dalam tugas akhir ini hanya dapat melakukan servis *instant messaging.* Sedangkan servis yang disediakan oleh Yahoo! cukup banyak, seperti conference, file transfer, dan lain – lain. Diharapkan pengembangan perangkat lunak selanjutnya agar dapat menambahkan fitur – fitur tersebut.
2. Pada perangkat lunak tidak disediakan fitur untuk melakukan pertukaran kunci, sehingga apabila user melakukan pertukaran kunci melalui media tertentu masih dapat diketahui oleh seorang *attacker.* Diharapkan pada pengembangan selanjutnya sistem dapat dilengkapi dengan perpaduan antara metode kriptografi simetris dan asimetris untuk melakukan pertukaran kunci dengan aman dan efisien.

DAFTAR PUSTAKA

[1] Adhitya Randy, *Study dan Perbandingan Algoritma Blowfish dan Twofish*, [pdf], didownload pada tanggal 29 Oktober 2011.

[2] Bruce Schneier, *Another New AES Attack*, [online], http://www.schneier.com/blog/archives/2009/07/another_new_aes.html, diakses pada tanggal 26 Oktober 2011.

[3] Bruce Schneier, *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)*, [Online], http://www.schneier.com/paper-blowfish-fse.html, diakses pada tanggal 18 Juni 2011.

[4] Bruce Schneier, *The Blowfish Encryption Algorithm -- One Year Later*, [online], http://www.schneier.com/paper-blowfish-oneyear.html, diakses pada tanggal 26 Oktober 2011.

[5] Dani, *Algoritma Twofish Sebagai Finalis AES dan Metode Kriptanalisisnya*, [pdf], didownload pada tanggal 1 September 2011.

[6] Federal Information Processing Standards (FIPS), *Announcing The Advance Encryption Standard (AES)*, [pdf], didownload pada tanggal 29 Oktober 2011.

[7] Joan Daemen, Vincent Rijmen, *A Specification for Rijndael The AES Algorithm*, [pdf], didownload pada tanggal 20 September 2011.

[8] Mohamad Octamanullah, *Perbandingan Algoritma Kriptografi Kunci Simetrik Blowfish dan Twofish*, [pdf], didownload pada tanggal 25 Oktober 2011.

[9] Munir Renaldi (2006). Kriptografi. Bandung : Penerbit Informatika.

[10] Willy Setiawan, *Analisa dan Perbandingan Algoritma Twofish dan Rijndael*, [pdf], didownload pada tanggal 29 Oktober 2011.