

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan dan kerahasiaan informasi merupakan hal yang sangat penting bagi suatu individu, organisasi ataupun perusahaan. Suatu data atau informasi akan memiliki nilai yang lebih tinggi jika menyangkut tentang aspek-aspek bisnis, keamanan ataupun kepentingan umum. Informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan didalamnya. Terlebih lagi dengan perkembangan teknologi informasi dewasa ini, yang memberikan kemudahan bagi kita untuk melakukan komunikasi dan pertukaran informasi melalui internet. Hal ini juga dapat meningkatkan tindakan kejahatan komputer yang dapat dilakukan melalui teknologi yang biasa disebut dengan istilah *cybercrime*, seperti penyadapan, pencurian ataupun perusakan data atau informasi.

Untuk melindungi dan menjaga kerahasiaan informasi agar terhindar dari tindakan-tindakan kejahatan komputer oleh orang-orang yang tidak berhak, maka salah satu cara yang dapat dilakukan adalah dengan memanfaatkan teknik enkripsi. Menurut Microsoft, enkripsi adalah nama yang diberikan untuk proses penerapan algoritma pada sebuah informasi, dimana proses tersebut akan mengacak data di dalamnya sehingga sangat sulit dan memakan waktu jika data hasil enkripsi tersebut dipecahkan tanpa mengetahui kode/sandi khusus. Dengan bantuan metode enkripsi, jika ada pihak ketiga menyadap dan mengambil informasi tersebut maka informasi tersebut tidak dapat dibaca, karena informasi tersebut sudah teracak yang pastinya akan sulit dimengerti oleh pihak yang tidak diinginkan.

Salah satu metode enkripsi adalah enkripsi RC6. RC6 adalah algoritma kriptografi *symmetric-key* yang merupakan perkembangan dari algoritma RC5 yang disertakan dalam *Advances Encryption Standard* (AES). RC6 menggunakan esensi dari *data-dependent rotations*. RC6 adalah algoritma yang menggunakan ukuran blok hingga 128 bit dan ukuran kunci yang digunakan bervariasi antara 128, 192 dan 256 bit. RC6 memecah blok 128 bit menjadi 4 buah blok 32 bit dengan mengikuti aturan enam operasi dasar yaitu : penjumlahan, pengurangan,

exclusive OR, perkalian bilangan integer, geser bit ke kanan, dan geser bit ke kiri. Proses utama dalam algoritma RC6 adalah penjadwalan kunci, dan proses enkripsi dekripsi [1]. Berdasarkan proses-proses tersebutlah, RC6 merupakan algoritma yang kuat dengan implementasi yang mudah dan cepat. RC6 salah satu kandidat AES dan meraih juara kedua. Untuk RC6 dengan 15 ronde atau kurang, berjalan pada inputan blok 128 bit, menunjukkan cipertext yang dihasilkan dapat berbeda dari sejumlah random bit. Beberapa aplikasi pemeriksa untuk keacakan bit *stream* menunjukkan hasil enkripsi yang kuat. Selain itu, penulis dari algoritma menunjukkan serangan terhadap RC6 berjalan lebih cepat dari *exhaustive key search*. Untuk satu kelas kunci lemah menunjukkan bahwa keacakan penuh tidak dicapai hingga 17 ronde algoritma. Algoritma RC6 adalah tahan terhadap *differential*, *cryptanalysis*, dengan syarat lebih dari 12 putaran. [2]

Namun teknik enkripsi memiliki kelemahan, yaitu pesan acak yang dikirim justru dapat menimbulkan kecurigaan oleh pihak luar, sehingga pesan tersebut dapat dirusak dengan tujuan agar pihak penerima yang asli tidak berhasil mendapatkan pesan tersebut secara utuh. Untuk mengatasi hal ini, dapat digunakan teknik lain, yaitu steganografi. Steganografi adalah ilmu pengetahuan dan seni dalam menyembunyikan informasi. Steganografi sedemikian rupa menyembunyikan isi suatu informasi di dalam suatu media yang tidak dapat di duga oleh orang biasa sehingga tidak menimbulkan suatu kecurigaan kepada orang yang melihatnya. Media untuk menyembunyikan informasi adalah (1) *Format image* diantaranya *bitmap* (bmp) , gif, pcx, dan jpeg (2) *Format audio* antara lain wav, mp3, voc (3) *Format lain* misalkan teks, doc, html dan pdf. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah informasi [3].

Salah satu metode steganografi adalah steganografi *whitespace*. Steganografi *whitespace* adalah teknik menyembunyikan informasi ke dalam teks dengan memanfaatkan karakter tab dan spasi (karakter *whitespace*) untuk mengkodekan data yang akan disembunyikan ke dalam teks [4]. Keunggulan dari jenis steganografi ini adalah visualiasi pesan tidak dapat dilihat secara kasat mata sehingga tidak menimbulkan kecurigaan saat informasi tersebut mengandung suatu pesan rahasia.

Dengan melakukan kombinasi antara enkripsi RC6 dan steganografi *whitespace* diharapkan dapat menghasilkan perlindungan

yang lebih baik bagi pesan/informasi, yaitu dengan mengenkripsikan pesan terlebih dahulu dengan enkripsi RC6, lalu menyembunyikan pesan yang telah dienkripsi dengan teknik steganografi *whitespace*. Berdasarkan permasalahan di atas, maka akan dilakukan penelitian yang membahas tentang aplikasi steganografi pada teks menggunakan metode *whitespace* dan enkripsi RC6. Kerahasiaan ditingkatkan dengan melakukan enkripsi informasi yang akan disisipkan menggunakan algoritma *Rivest Code 6 (RC6)*.

1.2 Rumusan Masalah

Dari latar belakang masalah di atas permasalahan yang dikaji yaitu

1. Seberapa aman hasil enkripsi RC6 terhadap teks yang diukur menggunakan *avalanche effect*.
2. Berapa nilai kompleksitas waktu Big Oh untuk algoritma RC6 dan steganografi *whitespace*.

1.3 Tujuan dan Manfaat

1.3.1 Tujuan

Tujuan dari penelitian ini yaitu :

1. Untuk mengetahui seberapa aman hasil enkripsi RC6 terhadap teks yang diukur menggunakan *avalanche effect*
2. Untuk mengetahui nilai kompleksitas waktu Big Oh untuk algoritma RC6 dan steganografi *whitespace*

1.3.2 Manfaat

Penelitian ini diharapkan mampu menjadi sebuah solusi dalam mengamankan teks untuk dijaga kerahasiannya dengan cara mengkombinasi metode steganografi *whitespace* dan enkripsi RC6.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

1. Data yang diproses adalah teks.
2. Tidak membaca file teks.
3. Inputan teks langsung dari *keyboard*.
4. Kunci yang digunakan pada algoritma sebesar 128 bit.
5. Parameter yang digunakan adalah Big Oh dan *Avalanche Effect*.

1.5 Metode Penelitian

Penelitian ini menerapkan beberapa metode penelitian sebagai berikut:

1. Studi Literatur

Pada tahap ini dilakukan pengumpulan referensi yang diperlukan dalam penelitian. Hal ini dilakukan untuk memperoleh informasi dan data yang diperlukan untuk penulisan skripsi ini. Referensi yang digunakan dapat berupa buku, jurnal, artikel, situs internet, maupun penelitian terdahulu yang berkaitan dengan penelitian ini.

2. Analisis sistem

Tahap ini digunakan untuk mengolah data dari hasil studi literatur yang kemudian dilakukan analisis terhadap proses kerja penyembunyian dan enkripsi pesan dengan menggunakan steganografi *whitespace* dan enkripsi RC6.

3. Perancangan sistem

Setelah tahapan analisis selesai, maka usulan kebutuhan akan diterjemahkan menjadi sistem informasi berbasis komputer, yaitu dengan membuat perancangan sistem. Pada tahap ini akan dibuat rancangan sistem seperti bagan alir sistem dan desain antar muka pengguna.

4. Analisis dan Implementasi

Implementasi dilakukan dengan menampilkan ke *user* hasil berupa aplikasi yang dapat mengamankan data teks dengan menggunakan steganografi *whitespace* dan enkripsi RC6 yang telah diimplementasikan ke dalam bahasa pemrograman Java.

5. Pengujian

Pada tahap ini dilakukan pengujian aplikasi untuk mengetahui apakah aplikasi sudah berjalan sesuai dengan tujuan penelitian atau tidak serta melakukan perbaikan jika masih terdapat *error* pada aplikasi.

Parameter yang digunakan dalam menguji sistem adalah :

1. Big Oh

Kecanggihan suatu program bukan dilihat dari tampilan program, melainkan berdasarkan efisiensi algoritma yang terdapat didalam program tersebut [5] . Efisiensi berarti algoritma tersebut dapat dijalankan untuk ukuran masukan tertentu dengan waktu yang diperlukannya tumbuh dengan tidak drastis. Ukuran efisiensi waktu eksekusi program dihitung dari *source code* program menggunakan nilai kompleksitas waktu asimptotik Big Oh.

2. *Avalanche Effect*

Untuk menentukan nilai *Avalanche Effect* dapat dilakukan dengan dua cara yaitu pertama menggunakan dua buah plainteks yang berbeda satu bit dengan dua kunci yang sama dan yang kedua menggunakan dua buah kunci yang berbeda satu bit dengan dua buah plainteks yang sama. Pengujian dilakukan pada sebuah teks dengan membandingkan jumlah bit yang berbeda pada *chipertext* yang dihasilkan dan seberapa besar perbedaan yang diakibatkan satu bit tersebut pada *Avalanche Effect*.

6. Dokumentasi dan Laporan Akhir

Pada tahap ini dilakukan dokumentasi hasil analisa dan perancangan yang digunakan untuk menuangkan hasil penelitian tersebut ke dalam laporan akhir dalam bentuk skripsi.

1.6 Sistematika Penulisan

Dalam penelitian ini, sistematika penulisan yang digunakan terbagi menjadi lima bab dengan susunan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini menjelaskan dasar-dasar dari penulisan laporan tugas akhir, yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan, metode penelitian serta sistematika penulisan laporan tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini membahas teori-teori yang berhubungan dengan topic penelitian, meliputi steganografi dan kriptografi

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas tentang analisis proses enkripsi dan dekripsi algoritma *RC6* dan steganografi *whitespace* yang terdiri dari *Flowchart* dan perancangan *User Interface*.

BAB 4 IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang hasil implementasi dan pengujian sistem serta pembahasan dari hasil yang diperoleh sesuai dengan analisis dan perancangan sistem yang dilakukan sebelumnya.

BAB 5 PENUTUP

Bab ini membahas tentang kesimpulan yang diperoleh dari hasil penelitian serta saran-saran yang ditujukan bagi para pembaca dan pengembang sistem untuk penelitian selanjutnya.