BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan pesatnya perkembangan teknologi Internet seperti sekarang ini, jumlah informasi yang dikirim dan diterima secara elektronik juga meningkat. Begitu juga dengan masalah keamanannya yang sudah banyak dibicarakan secara luas. Mengirim pesan terenkripsi sering akan menarik perhatian pihak ketiga, yaitu *cracker* dan *hacker*, sehingga akan terjadi upaya untuk memecahkan dan mengungkapkan pesan aslinya. Dalam dunia *digital*, steganografi diperkenalkan untuk menyembunyikan keberadaan komunikasi dengan menyembunyikan pesan rahasia di dalam pesan lain yang tidak dicurigai.

Skema penyembunyian informasi sudah lama dikenal, Julius Caesar menggunakan kriptografi untuk mengkodekan arahan politik (Singh et al, 2009). Steganografi (biasanya disebut sebagai stego), seni menulis tersembunyi, juga telah digunakan selama beberapa generasi. Steganografi sering sulit dibedakan dengan kriptografi karena kemiripan fungsi kedua bidang tersebut dalam hal melindungi informasi yang penting. Perbedaan antara kedua bidang adalah dalam hal cara melindungi informasi. Steganografi menyamarkan informasi pada media lain sehingga orang tidak merasakan keberadaan informasi tersebut (Aboalsamh et al, 2008). Sementara itu kriptografi melindungi data dengan cara mengubah informasi ke bentuk yang tidak bisa dibaca atau dimengerti oleh orang yang tidak berhak (Zaidan et al, 2009).

Tujuan utama steganografi adalah untuk menyembunyikan informasi di dalam media yang ditutupi sehingga orang luar tidak akan menemukan informasi yang terkandung didalamnya (Shahreza, 2006). Sebagian besar implementasi steganografi dilakukan pada citra (Zaidan et al, 2009; Bandyopadhyay et al, 2010) dan suara (Atoum et al, 2011). Pendekatan sederhana untuk penyisipan informasi pada media citra maupun suara adalah dengan cara menyisipkan pesan ke dalam bit rendah (*Least Significant Bits*/LSB) pada data piksel yang menyusun berkas citra BMP 24 bit atau di antara frame (BF) dalam berkas MP3 (Nosrati, 2011). Steganografi pada teks adalah jenis yang paling sulit dari steganografi yang lain (Shahreza, 2006), hal ini terutama disebabkan oleh terbatasnya *redundant bits* dalam sebuah berkas teks dibandingkan dengan citra atau berkas suara (Memon et al, 2008).

Steganografi sering digunakan bersamaan dengan kriptografi sehingga menawarkan privasi dan keamanan yang lebih tinggi melalui saluran komunikasi (Por et al,2008). Ada dua jenis algoritma kriptografi berdasarkan kunci yang dipakai untuk enkripsi dan dekripsi (Menezes et al, 1996), yaitu algoritma kunci rahasia (algoritma simetris) dan algoritma kunci publik (algoritma asimetris). Penggunaan algoritma kunci publik lebih banyak disarankan karena dapat mengatasi distribusi kunci yang menjadi masalah pada algoritma kunci rahasia. RSA adalah salah satu yang populer dari beberapa kriptografi kunci publik. Keamanan algoritma ini terletak pada sulitnya faktorisasi bilangan bulat komposit yang besar (Thome, 2009).

Ide untuk menyisipkan pesan rahasia ke dalam sebuah berkas CSS (*Cascading Style Sheet*) adalah terinspirasi dari penelitian yang dilakukan oleh Por dan Delina (2008). Penyembunyian pesan dapat diterapkan pada berkas CSS dengan menyisipkan pesan pada tiap *property style* CSS, yaitu setelah karakter *semicolon*. Lebih tepatnya menggunakan metode "*End of Line Spacing"* yaitu pemanfaatan *whitespace* untuk menyandikan data dengan memasukkan spasi maupun tab pada akhir baris *property* CSS. Sebuah pendekatan baru pengiriman pesan tanpa takut pesan dicegat dan kemudian diubah oleh pihak ketiga lalu mengirimkan pesan palsu kepada penerima. Penggunaan RSA sebagai salah satu algoritma kriptografi kunci publik juga dapat memberi keamanan ganda agar pesan sulit untuk dipecahkan. Penggunaan kriptografi kunci publik pada teknik steganografi juga pernah dilakukan oleh Bandyopadhyay pada penelitiannya yang lain (Bandyopadhyay and Parui, 2010), namun menggunakan citra sebagai media penutupnya.

1.1.1 Rumusan masalah

Berdasarkan latar belakang permasalahan tersebut diatas maka dapat diambil rumusan masalah sebagai berikut :

1. Bagaimana menyisipkan informasi rahasia melalui *Cascading Style Sheet* sebuah situs sebagai salah satu bentuk implementasi steganografi teks.
2. Bagaimana sistem kriptografi kunci publik dapat diterapkan pada skema steganografi teks yang disisipkan pada *Cascading Style Sheet* sebuah situs.
3. Bagaimana menganalisa kelebihan dan kelemahan dari skema ini.

1.1.2 Batasan Masalah

Batasan masalah pada penelitian ini adalah :

1. Implementasi dari metode yang dikembangkan ini menggunakan bahasa pemrograman PHP (berbasis web).
2. Sistem kriptografi kunci publik yang digunakan adalah algoritma kriptografi RSA.
3. Sampel yang disisipkan berupa teks serta memiliki ukuran yang sesuai dengan media penutup (*cover*).
4. Prototipe perangkat lunak sebagai bentuk implementasi dari skema yang diusulkan hanya dijalankan pada lingkungan *localhost*.

1.1.3 Manfaat Penelitian

Manfaat yang diharapkan pada penelitian ini adalah untuk pengembangan steganografi pada berkas teks khususnya pada berkas CSS (*Cascading Style Sheet*) dengan menggunakan metode penyisipan EOL (*End of Line*) yang dienkripsi menggunakan algoritma kriptografi RSA (*Rivest Shamir Adleman*). Manfaat lainnya adalah sebagai referensi dalam bidang kriptografi dan steganografi, khususnya pada bidang steganografi teks yang masih jarang ditemukan.

1.1.4 Keaslian Penelitian

Penelitian tentang steganografi pada media teks masih jarang ditemukan, hal ini dikarenakan sulitnya mencari ruang untuk disisipkan pada teks itu sendiri. Beberapa steganografi teks memanfaatkan *whitespace* sebagai ruang untuk

penyisipan, namun hal ini membuat struktur teks menjadi tak teratur dan berresiko diketahui oleh pihak ketiga. Pada penelititan ini akan dilakukan pengembangan dari metode *whitespace* yang cocok untuk diterapkan pada berkas CSS, dan menggabungkannya dengan algoritma kriptografi kunci publik RSA. Penggunaan metode *End of Line Spacing* diharapkan akan menghasilkan stegoteks yang mirip dengan aslinya dan tidak mengubah struktur teks yang ada. Berdasarkan studi literatur dari beberapa jurnal ilmiah, buku, artikel dan penelitian yang pernah dilakukan, belum ditemukan buku, artikel atau penelitian yang secara khusus membahas penerapan dari metode hibrid ini pada berkas CSS.

1.2 Tujuan Penelitian

Adapun tujuan penelitian yang ingin dicapai adalah :

1. Mengembangkan suatu skema penyisipan informasi yang dapat diterapkan pada berkas *Cascading Style Sheet* sebuah situs sebagai salah satu bentuk implementasi steganografi teks.
2. Menerapkan sistem kriptografi kunci publik pada skema steganografi teks yang disisipkan pada *Cascading Style Sheet* sebuah situs.
3. Menganalisa kelebihan dan kelemahan dari pengembangan metode yang diusulkan.

1.3 Hipotesis

Penggunaan metode *"End of Line Spacing"* pada skema ini akan membuat media penutup tak mengalami perubahan struktur atau sama seperti aslinya. Panjang kunci yang dipilih akan mempengaruhi jumlah karakter yang dapat ditampung oleh media penutup dalam hal ini CSS.

1.4 Sistematika Penulisan

Dokumen tugas akhir ini terdiri dari enam bab, yaitu :

BAB I PENDAHULUAN

Bab ini memuat latar belakang masalah, rumusan masalah, batasan masalah, manfaat yang diharapkan dari penelitian ini, tujuan penelitian serta sistematika penulisan laporan.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan dijelaskan mengenai uraian tinjauan pustaka dan landasan teori yang digunakan penulis. Tinjauan pustaka beberapa referensi yang berkaitan dengan Steganografi dan Kriptografi. Landasan teori memuat tentang metode-metode steganografi dan kriptografi yang digunakan.

BAB III METODOLOGI PENELITIAN

Bab ini memuat cara penelitian secara rinci mulai dari pendekatan penelitian, tahapan dan prosedur penelitian, hingga prosedur pengujian sistem.

BAB IV ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan dijelaskan mengenai tahap-tahap perancangan perangkat lunak yang akan dibuat. Mulai dari gambaran sistem secara lengkap, pembahasan metode-metode yang digunakan, hingga perancangan sistem.

BAB V IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini akan diuraikan mengenai gambaran peng-implementasi-an sistem. Selain itu akan disertakan pula dengan hasil pengujian perangkat lunak.

BAB VI PENUTUP

Bab ini berisi tentang kesimpulan secara keseluruhan dan saran yang dapat diambil dari penelitian yang telah dilakukan.