

TESIS

**SKEMA KEAMANAN STEGANOGRAFI
PADA *CASCADING STYLE SHEET* MENGGUNAKAN
SISTEM KRIPTOGRAFI KUNCI PUBLIK**



HERMAN KABETTA
No. Mhs.: 105301476/PS/MTF

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA
PROGRAM PASCASARJANA
UNIVERSITAS ATMA JAYA YOGYAKARTA
2012



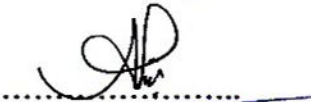
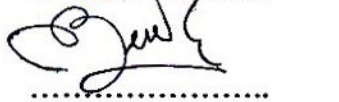
UNIVERSITAS ATMA JAYA YOGYAKARTA

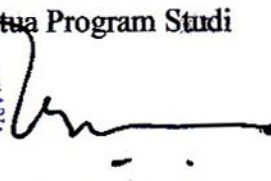
PROGRAM PASCA SARJANA

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

HALAMAN PENGESAHAN

Nama : Herman Kabetta
Nomor Mahasiswa : 105301476 / PS / MTF
Konsentrasi : Soft Computing
Judul Tesis : Skema Keamanan Steganografi pada *Cascading Style Sheet* Menggunakan Sistem Kriptografi Kunci Publik

Nama Pembimbing/Penguji	Tanggal	Tanda tangan
B. Yudi Dwiandiyanta, S.T., M.T.	17-10-2012	
Prof. Suyoto, M.Sc., Ph.D.	17-10-2012	
Dr. Pranowo, S.T., M.T.	17-10-2012	


Ketua Program Studi

PROGRAM PASCASARJANA
Dra. Ernawati, M.T.

PERNYATAAN

Dengan ini, saya yang bertanda tangan di bawah ini:

Nama : Herman Kabetta
Nomor Mahasiswa : 105301476 / PS / MTF
Program Studi : Magister Teknik Informatika
Konsentrasi : Soft Computing
Judul Tesis : Skema Keamanan Steganografi pada *Cascading Style Sheet* Menggunakan Sistem Kriptografi Kunci Publik

Menyatakan bahwa penelitian ini adalah hasil karya pribadi dan bukan duplikasi dari karya tulis yang telah ada sebelumnya. Karya tulis yang telah ada sebelumnya dijadikan penulis sebagai acuan untuk melengkapi penelitian dan dinyatakan secara tertulis dalam daftar pustaka.

Demikian pernyataan ini dibuat untuk digunakan sebagaimana mestinya.

Yogyakarta, 25 September 2012

Herman Kabetta

INTISARI

Dalam beberapa tahun terakhir, dunia pemrograman telah diperkenalkan kepada bahasa pemrograman baru dalam hal perancangan situs web, yakni CSS, yang dapat digunakan bersama dengan HTML untuk pengembangan antarmuka situs web. Sekarang, kedua bahasa pemrograman tersebut seakan tak terpisahkan satu sama lain. Sebagai sebuah *client-side scripting*, kode sumber CSS dapat terlihat oleh semua pengguna sebagaimana naskah aslinya, namun tidak dapat diubah begitu saja. Situs web sebagai alat penyebar informasi ke seluruh dunia, tentu saja dapat digunakan untuk berkomunikasi secara rahasia dengan memanfaatkan CSS sebagai penyembunyi pesannya. Penelitian ini mengusulkan skema baru untuk menyembunyikan informasi dengan memanfaatkan berkas situs web seperti CSS. Mekanisme komunikasi rahasia ini menggunakan teknik steganografi teks dengan media penutup berupa berkas CSS yang digabungkan dengan menggunakan algoritma kriptografi kunci publik RSA sebagai sistem enkripsinya.

Hasil akhir dari penelitian ini menunjukkan bahwa informasi dapat disisipkan pada berkas CSS, dan maksimum informasi yang dapat ditampung oleh berkas penutup dimodelkan dengan persamaan yang lebih spesifik. Model persamaan juga telah dibuktikan melalui pengujian pada berkas CSS yang berisi 760 baris *semicolon*, dengan pemilihan bilangan p dan q yang bervariasi antara 5 hingga 40 digit angka, diperoleh rentang antara 56 hingga 72 karakter untuk maksimum informasi yang dapat ditampung.

Kata kunci : Steganografi Teks, Kriptografi, Cascading Style Sheet (CSS), Algoritma RSA, Algoritma Kunci Publik

ABSTRACT

In many recent years, the programming world has been introduced about a new programming language for designing websites, it is CSS that can be used together with HTML to develop a web interface. And now, these two programming languages as if inseparably from each other. As a client-side scripting, CSS is visible by all users as the original script, but it can not be granted changed. Website is a tool of information disseminator throughout the world, this is certainly can be used to a secret communication by using CSS as a message hider. This research proposed a new scheme using web tools like CSS for hiding the informations. This is a secret communication mechanism using text steganography techniques that is embedded messages on CSS files and is further encrypted using RSA as a public key cryptographic algorithm.

The final result shows that informations can be embedded on CSS, and the maximum amount of informations have been modeled with a specific equation. The equations have also been proved by testing on the CSS file which contains 760 rows semicolon, with the numbers selection of p and q with varying digit between 5 to 40 digit numbers, its obtained varying ranges between 56 to 72 characters for the maximum information that can be stored.

Keywords : *Text Steganography, Cryptography, Cascading Style Sheet (CSS), RSA Algorithm, Public Key Algorithm*

KATA PENGANTAR

Puji syukur atas kehadiran ALLAH SWT Tuhan Yang Maha Kuasa yang telah memberikan hidayah dan petunjuk-Nya sehingga penulis diberikan kesempatan, kesehatan dan kenikmatan hingga dapat menyelesaikan tesis dengan judul “Skema Keamanan Steganografi pada *Cascading Style Sheet* Menggunakan Sistem Kriptografi Kunci Publik”. Tesis ini dibuat sebagai salah satu syarat untuk memperoleh gelar kesarjanaan tingkat strata dua (S2) di Program Studi Magister Teknik Informatika Universitas Atma Jaya Yogyakarta.

Penulisan tugas akhir ini tidak terlepas dari peran serta banyak pihak yang telah membantu dari awal penelitian hingga selesai. Untuk itu, dengan segala hormat penulis mengucapkan terima kasih kepada :

1. Kedua Orang Tua ku, Ayahku Slamet Suherman, S.Pd. dan Ibuku Megawati, yang selalu mendoakan kebaikan dan keberhasilan untukku.
2. Bapak B. Yudi Dwiandiyanta S.T., M.T., selaku Dosen Pembimbing I dan Bapak Prof. Suyoto, M.Sc., Ph.D. selaku Dosen Pembimbing II yang sudah banyak meluangkan waktu dan kesempatannya untuk membimbing dengan memberikan arahan dan masukan terkait Tugas Akhir Penulis, serta Bapak Dr. Pranowo, S.T., M.T. selaku dosen penguji, terima kasih atas segala saran dan masukannya.
3. Kedua Saudaraku, Kakakku Herman Katoppo yang selalu mengerti apa yang ada dalam pikiranku dan Adikku Herman Arya Sadewa yang selalu setia menemani bermain dikala penat.

4. Kekasih hatiku mEMi, Dhama Peni Lasari, seseorang yang memiliki mimpi-mimpi hebat, yang selalu memberikan semangat dikala asa meredup, dan yang selalu meyakinkanku bahwa aku mampu, terima kasih atas doa-doa dan semua waktu bersamamu.
5. Teman-teman MTF angkatan September 2010 dan Januari 2011, terima kasih telah memberikan masa-masa yang membuatku tak merasa tua. Terkhusus untuk sahabatku Selus Kelin, thanks buat pinjaman printernya bro, maaf menghabiskan banyak tinta, hehehe.
6. Segenap Dosen Program Pascasarjana Magister Teknik Informatika yang tidak bisa disebutkan satu persatu, terima kasih atas ilmu yang diberikan, semoga ilmu yang didapat penulis dapat bermanfaat.
7. Semua pihak yang tidak bisa penulis sebutkan satu persatu, terima kasih dan salam sukses bagi kita semua, semoga segala amal kebaikan dibalas berlipat ganda oleh Tuhan Yang Maha Esa. Amin.

Tak ada gading yang tak retak, karena kesempurnaan hanyalah milik Tuhan Yang Maha Esa, namun sekiranya hasil penelitian yang penulis sajikan ini dapat mendekati harapan kesempurnaan. Harapan penulis, semoga penelitian ini membawa manfaat bagi agama, bangsa dan negara.

Yogyakarta, 25 September 2012

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN	iii
INTISARI	iv
ABSTRACT	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.1.1 Rumusan masalah	3
1.1.2 Batasan Masalah	4
1.1.3 Manfaat Penelitian	4
1.1.4 Keaslian Penelitian	4
1.2 Tujuan Penelitian	5
1.3 Hipotesis	6
1.4 Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA	8
2.1 Tinjauan Pustaka	8
2.2 Landasan Teori	12
2.2.1 Steganografi	12
2.2.2 Media Steganografi	13
2.2.3 Teori Bilangan	17
2.2.3.1 Modulo	18
2.2.3.2 Bilangan Prima	18
2.2.3.3 <i>Greatest Common Divisor</i> dan Bilangan Prima Relatif	19
2.2.3.4 Fungsi Totient Euler (<i>Euler Totient Function</i>)	20
2.2.4 Kriptografi	20
2.2.4.1 Terminologi dalam Kriptografi	21
2.2.4.2 Algoritma Kriptografi	22

2.2.4.3	Algoritma RSA (Rivest, Shamir, Adleman)	25
2.2.5	Cascading Style Sheet (CSS)	28
2.2.6	Hypertext Preprocessor (PHP)	29
BAB III	METODOLOGI PENELITIAN	31
3.1	Pendekatan Penelitian	31
3.2	Tahapan dan Prosedur Penelitian	31
3.2.1	Studi dan Analisa	32
3.2.1.1	Pengumpulan Data	32
3.2.1.2	Analisis Data Dokumentasi	33
3.2.2	Analisis Kebutuhan Sistem	33
3.2.3	Desain Sistem	34
3.2.3.1	Perancangan Sistem	34
3.2.3.2	Implementasi (<i>coding</i>)	35
3.2.3.3	Pengujian Sistem	35
BAB IV	ANALISIS DAN PERANCANGAN SISTEM	36
4.1	Gambaran Sistem	36
4.2	Penggunaan Algoritma RSA	37
4.2.1	Prosedur Pembangkitan Pasangan Kunci	39
4.2.2	Prosedur Enkripsi	41
4.2.3	Prosedur Dekripsi	44
4.3	Penggunaan Metode <i>End of Line Spacing</i>	45
4.3.1	Metode Konversi	46
4.3.2	Algoritma Proses Penyisipan (<i>Embedding</i>)	50
4.3.3	Algoritma Proses Ekstraksi (<i>Extracting</i>)	51
4.4	Perancangan Sistem	52
4.4.1	<i>Data Flow Diagram</i> (DFD)	53
4.4.2	Perancangan Antarmuka	58
4.4.2.1	Antarmuka Halaman Menu Utama (Home)	58
4.4.2.2	Antarmuka Halaman Pembangkitan Kunci	59
4.4.2.3	Antarmuka Halaman Penyisipan (<i>Embedding</i>)	60
4.4.2.4	Antarmuka Halaman Hasil Penyisipan (<i>Embedding</i>)	62
4.4.2.5	Antarmuka Halaman Ekstraksi (<i>Extracting</i>)	63
BAB V	IMPLEMENTASI DAN PENGUJIAN SISTEM	65
5.1	Implementasi Sistem	65

5.1.1 Implementasi Antarmuka	67
5.1.1.1 Halaman Utama (<i>Home</i>)	67
5.1.1.2 Halaman Pembangkitan Kunci (<i>Generate Keys</i>)	68
5.1.1.3 Halaman Penyisipan	69
5.1.1.4 Halaman Ekstraksi	70
5.1.2 Implementasi Fungsi-Fungsi	71
5.1.2.1 Implementasi Fungsi Pembangkit Kunci	72
5.1.2.2 Implementasi Fungsi Pengecekan Maksimum Karakter ..	73
5.1.2.3 Implementasi Fungsi Enkripsi	75
5.1.2.4 Implementasi Fungsi Dekripsi	76
5.1.2.5 Implementasi Fungsi Konversi	77
5.1.2.6 Implementasi Fungsi <i>Embedding</i>	80
5.1.2.7 Implementasi Fungsi <i>Extracting</i>	81
5.2 Pengujian Sistem	82
5.2.1 Pengujian Proses Pembangkitan Kunci	82
5.2.2 Pengujian Proses <i>Embedding</i>	84
5.2.2.1 Pengujian Maksimum Karakter	84
5.2.2.2 Pengujian Proses Enkripsi	89
5.2.2.3 Pengujian Proses <i>Encoding</i> dan <i>Embedding</i>	91
5.2.3 Pengujian Proses <i>Extracting</i>	93
5.2.3.1 Pengujian Proses <i>Extracting</i> dan <i>Decoding</i>	94
5.2.3.2 Pengujian Proses Dekripsi	95
5.3 Evaluasi Ketahanan (<i>Robustness</i>)	96
BAB VI PENUTUP	98
6.1 Kesimpulan	98
6.2 Saran	99
DAFTAR PUSTAKA	100
LAMPIRAN	

DAFTAR TABEL

Tabel 2.1 Tabel Pembanding Penelitian	10
Tabel 4.1 Konversi Plainteks ASCII menjadi Kode Desimal	41
Tabel 4.2 Konversi Plainteks Desimal menjadi Karakter ASCII	45
Tabel 4.3 Proses konversi cipherteks Desimal menjadi Biner	48
Tabel 4.4 Proses konversi cipherteks Biner menjadi Desimal	50
Tabel 4.5 Deskripsi Objek Halaman Utama.....	59
Tabel 4.6 Deskripsi Objek Halaman Pembangkitan Kunci	60
Tabel 4.7 Deskripsi Objek Halaman Penyisipan.....	61
Tabel 4.8 Deskripsi Objek Halaman Hasil Penyisipan.....	63
Tabel 4.9 Deskripsi Objek Halaman Ekstraksi.....	64
Tabel 5.1 Hasil implementasi aplikasi sistem steganografi	65
Tabel 5.2 Pengujian Maksimum Karakter Dengan Nilai p dan q Acak.....	87
Tabel 5.3 Pengujian Maksimum Karakter Dengan Nilai p dan q Maksimum	89
Tabel 5.4 Pengujian proses <i>encoding</i>	92

DAFTAR GAMBAR

Gambar 2.1 Proses Steganografi	12
Gambar 2.2 Diagram tipe media steganografi.....	13
Gambar 2.4 Skema kriptografi simetris	23
Gambar 2.5 Skema kriptografi asimetris.	24
Gambar 3.1 Tahapan Penelitian.....	32
Gambar 4.1 Gambaran sistem Steganografi CSS.....	36
Gambar 4.2 Diagram alir proses konversi dan penyamaran	47
Gambar 4.3 Diagram alir proses konversi dan pengungkapan (<i>revealing</i>).....	49
Gambar 4.4 Diagram alir algoritma penyisipan (<i>embedding</i>).....	51
Gambar 4.5 Diagram alir algoritma ekstraksi (<i>extracting</i>)	52
Gambar 4.6 Diagram Konteks Sistem Steganografi.....	53
Gambar 4.7 DFD level 1 sistem steganografi	54
Gambar 4.9 DFD level 3 Proses Ekstraksi Pesan.....	56
Gambar 4.10 DFD level 2 Sistem Pengirim.....	57
Gambar 4.11 Rancangan Antarmuka Halaman Utama.....	58
Gambar 4.12 Rancangan Antarmuka Halaman Pembangkitan Kunci.....	59
Gambar 4.13 Rancangan Antarmuka Halaman Penyisipan	61
Gambar 4.14 Rancangan Antarmuka Halaman Hasil Penyisipan	62
Gambar 4.15 Rancangan Antarmuka Halaman Ekstraksi.....	63
Gambar 5.1 Halaman Utama (<i>Home</i>)	67
Gambar 5.2 Halaman Pembangkitan Kunci	68
Gambar 5.3 Halaman Penyisipan	69
Gambar 5.4 Halaman Hasil Penyisipan	70
Gambar 5.5 Halaman Ekstraksi.....	71
Gambar 5.6 Implementasi Fungsi Pembangkit Kunci Pada PHP.....	73
Gambar 5.7 Implementasi Fungsi Pengecekan Maksimum Karakter.....	75
Gambar 5.8 Implementasi Fungsi Enkripsi Pada PHP	76
Gambar 5.9 Implementasi Fungsi Dekripsi Pada PHP	77
Gambar 5.10 Implementasi Fungsi Konversi dari Decimal ke Biner.....	78
Gambar 5.11 Implementasi Fungsi Konversi dari Biner ke Decimal.....	79
Gambar 5.12 Implementasi Fungsi Penyamaran.....	79
Gambar 5.13 Implementasi Fungsi Pengungkapan (<i>Revealing</i>)	80
Gambar 5.14 Implementasi Fungsi <i>Embedding</i>	81

Gambar 5.15 Implementasi Fungsi <i>Extracting</i>	82
Gambar 5.16 Sampel teks pesan untuk pengujian.....	85
Gambar 5.17 Hasil pengujian dengan bilangan p dan q acak	86
Gambar 5.18 Hasil pengujian dengan bilangan p dan q maksimum	88
Gambar 5.19 Pengujian Proses <i>Embedding</i>	93
Gambar 5.20 Hasil pengujian proses dekripsi.....	95
Gambar 5.21 Berkas CSS Stego sebelum dikompresi.....	97
Gambar 5.22 Berkas CSS Stego setelah dikompresi.....	97

