

BAB VI

PENUTUP

6.1 Kesimpulan

Dari analisis hingga pengujian yang telah dilakukan pada penelitian ini, dapat ditarik beberapa kesimpulan sebagai berikut :

1. Salah satu implementasi steganografi teks untuk menyisipkan informasi pada berkas CSS adalah dengan menggunakan metode *End of Line Spacing*, metode ini menghasilkan berkas CSS stego yang sama seperti berkas penutup aslinya, atau dengan kata lain metode ini tidak merubah susunan karakter pada berkas penutup (*coverteks*).
2. Algoritma RSA yang telah ada dimodifikasi untuk memaksimalkan keterbatasan penampungan informasi pada berkas CSS. Pada penerapannya, algoritma enkripsi dirumuskan dengan persamaan,

$$C = \left(\sum_{i=1}^{\lfloor \frac{\lfloor \log(n) \rfloor}{2} \rfloor - \lfloor \frac{\lfloor \log(n) \rfloor}{10} \rfloor} (m_i \cdot 256^{i-1}) \right)^e \bmod n$$

sedangkan algoritma dekripsi dirumuskan dengan persamaan,

$$m_i = \left\lfloor \frac{C^d \bmod n}{256^{i-1}} \right\rfloor \bmod 256$$

3. Penggunaan algoritma kriptografi kunci publik RSA merupakan kelebihan dari skema ini, algoritma RSA akan mengenkripsi informasi sebelum disisipkan sehingga kemungkinan informasi diketahui oleh pihak ketiga akan lebih kecil.

4. Salah satu kelemahan dari skema ini adalah tindakan kompresi yang mengakibatkan hilangnya informasi yang terkandung dalam berkas CSS, namun kelemahan ini dapat diatasi dengan adanya otoritas pengelolaan pada *webserver*.
5. Panjang kunci yang dipilih tidak mempengaruhi jumlah karakter yang dapat ditampung oleh media penutup dalam hal ini berkas CSS. Jumlah karakter maksimum yang dapat ditampung oleh berkas CSS dirumuskan dengan persamaan berikut,

$$MKP = \left\lfloor \frac{JS}{4 \left(\left\lfloor \log \left(\left(\sum_{i=1}^{\left\lfloor \frac{[\log(n)]}{2} \right\rfloor - \left\lfloor \frac{[\log(n)]}{10} \right\rfloor} (255 * 256^{i-1}) \right)^e \text{ mod } n \right) \right\rfloor + 1} \right) \cdot \left(\left\lfloor \frac{[\log(n)]}{2} \right\rfloor - \left\lfloor \frac{[\log(n)]}{10} \right\rfloor \right) \right\rfloor$$

dengan *JS* adalah Jumlah dari *semicolon* yang terdapat pada berkas CSS.

6.2 Saran

Dalam penelitian ini, informasi yang disembunyikan bergantung pada jumlah karakter *semicolon* yang tersedia, sehingga kapasitas penampungan informasi menjadi terbatas. Pada pengembangan selanjutnya diharapkan kapasitas penampungan berkas dapat ditingkatkan serta adanya peningkatan ketahanan (*robustness*) terhadap tindakan kompresi.

DAFTAR PUSTAKA

- Aboalsamh, Hatim A., Hassan I. Mathkour , Mona F. M. Mursi and Ghazy M.R. Assassa, 2008, *Steganalysis of JPEG Images: An Improved Approach for Breaking the F5 Algorithm*. 12th WSEAS International Conference on COMPUTERS, Heraklion, Greece, July 23-25, 2008.
- Al-Vahed, Ahmed and Haddad Sahhavi, 2011, *An overview of modern cryptography*. World Applied Programming, Vol (1), No (1), April 2011.3-8.
- Atoum, Mohammed Salem, Mamoun Suleiman Al Rababaa, Subariah Ibrahim, and Osamah Abdulgader Ahmed, 2011, *A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III*. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011.
- Atoum, Mohammed Salem, Osamah Abdulgader Al- Rababah and Alaa Ismat Al-Attili, 2011, *New Technique for Hiding Data in Audio File*. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.4, April 2011.
- Bandyopadhyay, Samir Kumar, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, 2008, *A Tutorial Review on Steganography*. International Conference on Contemporary Computing 2008.

Bandyopadhyay, Samir Kumar and Sarthak Parui, 2010, *A Method for Public Key Method of Steganography*. International Journal of Computer Applications (0975 – 8887) Volume 6– No.3, September 2010.

Bandyopadhyay, Samir Kumara and Suman Chakraborty, 2011, *Image Steganography Using DNA Sequence*. Asian Journal Of Computer Science And Information Technology 1:2 (2011) 50 – 52.

Bandyopadhyay , Samir Kumar, Tuhin Utsab Paul and Avishek Raychoudhury, 2010, *Genetic Algorithm Based Substitution Technique Of Image Steganography*. Journal of Global Research in Computer Science Volume 1, No. 5, December 2010.

Banerjee, Indradip, Souvik Bhattacharyya and Gautam Sanyal, 2011, *Novel Text Steganography through Special Code Generation*. International Conference on Systemics, Cybernetics and Informatics 2011 Pentagram Research Centre (P) Limited.

Begum, M. Baritha and Y. Venkataramani, 2011, *LSB Based Audio Steganography Based On Text Compression*. International Conference on Communication Technology and System Design 2011.

Benedetto, E., 2009, *Arithmetical Approach To The Twin Primes Conjecture*. Annali Dell'universita di Ferrara, Volume 57, Number 1 (2011), 191-198, DOI: 10.1007/s11565-009-0070-8.

Carro, Fernando Incertis, 2007, *Methods of invisibly embedding and hiding data into soft-copy text documents*. U.S. Patent No. 7240209 B2 July 3rd 2007.

Crandall, Richard and Carl Pomerance, 2005, *Prime Numbers: A Computational Perspective*. Springer Science Business Media Inc.

Das, Soumyendu, Subhendu Das, Bijoy Bandyopadhyay, and Sugata Sanyal, 2008, *Steganography and Steganalysis: Different Approaches*. International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008.

Dutta, Poulami, Debnath Bhattacharyya, and Tai-hoon Kim, 2009, *Data Hiding in Audio Signal: A Review*. International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

Geetha, K and P.Vanitha Muthu, 2010, *Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy*. International Journal on Computer Science and Engineering Vol. 02, No. 04, 2010, 1308-1313.

Hamdi, Mohamed, 2010, *Architecture and Insecurity Issues of a Handheld Device*. Journal of Security Engineering Volume 6-2010.

<http://gmplib.org/> diakses tanggal 7 September 2012

<http://primes.utm.edu/> diakses tanggal 10 September 2012

<http://www.php.net> diakses pada tanggal 20 November 2011.

Jalab, Hamid.A., A.A Zaidan and B.B Zaidan, 2009, *Frame Selected Approach for Hiding Data within MPEG Video Using Bit Plane Complexity Segmentation*. Journal Of Computing, Volume 1, Issue 1, December 2009.

Jaseena and Anita John, 2011, *Text Watermarking using Combined Image and Text for Authentication and Protection*. International Journal of Computer Applications (0975 – 8887) Volume 20– No.4, April 2011.

Kabetta, Herman, B. Yudi Dwiandiyanta, Suyoto, 2011, *Information Hiding in CSS : A Secure Scheme Text-Steganography Using Public Key Cryptosystem*. International Journal on Cryptography and Information Security(IJCIS),Vol.1, No.1,November 2011

Keller, Matthias and Martin Nussbaumer, 2010, *CSS Code Quality: A Metric for Abstractness Or Why Humans Beat Machines in CSS Coding*. 2010 Seventh International Conference on the Quality of Information and Communications Technology.

Kumar, Vinay and S.K. Muttoo, 2008, *Relevance of Steganography, in General, and Graph Theoretic Approach in Particular, in Indian Security Concern and Measure*. National Conference of Computing For Nation Development, February 08-09, 2008.

Memon, Aasma Ghani, Sumbul Khawaja and Asadullah Shah, 2008, *Steganography: A New Horizon For Safe Communication Through XML*. Journal of Theoretical and Applied Information Technology 2008.

Memon, Jibrán Ahmed, Kamran Khowaja and Hameedullah Kazi, 2008, *Evaluation Of Steganography For Urdu /Arabic Text*. Journal of Theoretical and Applied Information Technology 2008.

Menezes , A ., P. van Oorschot, and S. Vanstone, 1996, *Handbook of Applied Cryptography*. CRC Press 1996.

Mir, Nighat and Sayed Afaq Hussain, 2010, *Secure web-based communication*. Procedia Computer Science 3 (2011) 556–562.

Narayana, Sujay and Gaurav Prasad, 2010, *Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions*. Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010.

Nosrati, Masoud, Ronak Karimi, Hamed Nosrati and Maryam Karimi, 2011, *An introduction to steganography methods*. World Applied Programming, Vol (1), No (1), April 2011, 37-41.

Por, L.Y., T. F. Ang and B. Delina, 2008, *WhiteSteg: A New Scheme in Information Hiding Using Text Steganography*. WSEAS Transactions on Computers Issue 6, Volume 7, June 2008.

Por, L.Y., W. K. Lai, Z. Alireza, T. F. Ang, M.T. Su, and B. Delina, 2008, *StegCure: A Comprehensive Steganographic Tool using Enhanced LSB Scheme*. WSEAS Transactions on Computers Issue 8, Volume 7, August 2008.

Por, L. Y. and B. Delina, 2008, *Information Hiding: A New Approach in Text Steganography*. 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (ACACOS '08), Hangzhou, China, April 6-8, 2008.

Quint, Vincent and Irne Vatton, 2007, *Editing with Style*. Proceedings of the 2007 ACM symposium on Document engineering. Winnipeg, Manitoba, Canada: ACM, 2007.

Radha, N., T. Rubya and S. Karthikeyan, 2011, *Securing Retinal Template Using Quasigroups*. Journal of Advances In Information Technology, Vol. 2, No. 2, May 2011.

Raskind, Wayne and Edward K. Blum, 2011, *Computer Security and Public Key Cryptography*. Computer Science : The Hardware, Software and Heart of It 2011, Part 2, 231-240, DOI: 10.1007/978-1-4614-1168-0_11.

Shahreza, M. Hassan Shirali and Muhammad Shirali Shahreza, 2006, *A New Approach to Persian/Arabic Text Steganography*. International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR'06).

- Singh, Hitesh, Pradeep Kumar Singh and Kriti Saroha, 2009, *A Survey on Text Based Steganography*. Proceedings of the 3rd National Conference, Computing For Nation Development, February 26 – 27, 2009.
- Stallings W., 1999, *Cryptography and Network Security Principles and Practice second edition*. Prentice Hall, New Jersey USA.
- Stamey, John, Bryan Saunders and Simon Blanchard, 2005, *The Aspect-Oriented Web*. Proceedings of the 23rd annual international conference on Design of communication: documenting & designing for pervasive information.
- Sulthana, E. S. Shameem and S.Kanmani, 2011, *Evidence based Access Control over Web Services using Multi Security*. International Journal of Computer Applications (0975 – 8887) Volume 17– No.3, March 2011.
- Sunyoto, Andi, 2007, *AJAX Membangun Web dengan Teknologi Asynchronous Javascript dan XML*. Penerbit Andi Yogyakarta, Indonesia.
- Supaartagorn, Chanchai, 2011, *PHP Framework For Database Management Based on MVC Pattern*. International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 2, April 2011.
- Thampi, Sabu M, 2004, *Information Hiding Techniques: A Tutorial Review*. ISTE-STTP on Network Security & Cryptography, LBSCE 2004.

Thome, Emmanuel, 2009, *Abstracts of the CADO workshop on integer factorization*. ACM Communications in Computer Algebra, Vol. 43, No. 1, March 2009.

Walia, Ekta, Payal Jain and Navdeep, 2010, *An Analysis of LSB & DCT based Steganography*. Global Journal of Computer Science and Technology Vol. 10 Issue 1 (Ver 1.0), April 2010.

Yin R, 2003, *Case study research: Design and Methods*. Third edition. Sage publications. Inc.

Zaidan, B.B, A.A. Zaidan, Alaa Taqa and Fazida Othman, 2009, *Stego-Image Vs Stego-Analysis System*. International Journal of Computer and Electrical Engineering, Vol. 1, No. 5 December, 2009.

Zou, Yejun, 2010, *A Java Based Software Solution For Efficient Pairing Cryptography*. Department of Computer Science, National University of Ireland Maynooth, Co. Kildare Ireland.

LAMPIRAN 1

ASCII CODE STANDARD AND EXTENDED

STANDARD ASCII (0-127)						EXTENDED ASCII (128-255)									
Control Codes		Keyboard and <Alt+number>				<Alt+number>									
0	Null	32	space	64	@	96	`	128	Ç	160	á	192	+	224	α
1	Start of heading	33	!	65	A	97	a	129	ü	161	í	193	-	225	β
2	Start of text (STX)	34	"	66	B	98	b	130	é	162	ó	194	-	226	Γ
3	End of text (ETX)	35	#	67	C	99	c	131	â	163	ú	195	+	227	π
4	End of transmit (EOT)	36	\$	68	D	100	d	132	ä	164	ñ	196	-	228	Σ
5	Enquiry (ENQ)	37	%	69	E	101	e	133	à	165	Ñ	197	+	229	σ
6	Acknowledge (ACK)	38	&	70	F	102	f	134	å	166	ª	198		230	μ
7	Audible bell (BEL)	39	'	71	G	103	g	135	ç	167	º	199		231	τ
8	Backspace (BS)	40	(72	H	104	h	136	ê	168	¿	200	+	232	Φ
9	Horizontal tab (HT)	41)	73	I	105	I	137	ë	169	¬	201	+	233	Θ
10	Line feed (LF)	42	*	74	J	106	j	138	è	170	¬	202	-	234	Ω
11	Vertical tab (VT)	43	+	75	K	107	k	139	ì	171	½	203	-	235	δ
12	Form feed (FF)	44	,	76	L	108	l	140	î	172	¼	204		236	∞
13	Carriage return (CR)	45	-	77	M	109	m	141	ï	173	ï	205	-	237	φ
14	Shift out (SO)	46	.	78	N	110	n	142	Ä	174	<<	206	+	238	ε
15	Shift in (SI)	47	/	79	O	111	o	143	Å	175	>>	207	-	239	∩
16	Data link escape	48	0	80	P	112	p	144	É	176		208	-	240	≡
17	Device control 1	49	1	81	Q	113	q	145	æ	177		209	-	241	±
18	Device control 2	50	2	82	R	114	r	146	Æ	178		210	-	242	≥
19	Device control 3	51	3	83	S	115	s	147	ô	179		211	+	243	≤
20	Device control 4	52	4	84	T	116	t	148	ö	180		212	+	244	(
21	Neg. acknowledge	53	5	85	U	117	u	149	ò	181		213	+	245)
22	Synchronous idle	54	6	86	V	118	v	150	û	182		214	+	246	÷
23	End trans. Block	55	7	87	W	119	w	151	ù	183	+	215	+	247	≈
24	Cancel (CAN)	56	8	88	X	120	x	152	ÿ	184	+	216	+	248	°
25	End of medium (EM)	57	9	89	Y	121	y	153	Ö	185		217	+	249	·
26	Substitution (SUB)	58	:	90	Z	122	z	154	Ü	186		218	+	250	·
27	Escape (ESC)	59	;	91	[123	{	155	ç	187	+	219		251	√
28	File separator (PS)	60	<	92	\	124		156	£	188	+	220	_	252	n
29	Group separator (GS)	61	=	93]	125	}	157	¥	189	+	221		253	²
30	Record separator (RS)	62	>	94	^	126	~	158	Ɔ	190	+	222		254	!
31	Unit separator (US)	63	?	95	_	127		159	f	191	+	223	-	255	

SKPL

SPEKIFIKASI KEBUTUHAN PERANGKAT LUNAK

SteganoCSS

Untuk : Tugas Akhir

Disusun oleh:

Herman Kabetta (105301476/PS/MTF)

Program Studi Magister Teknik Informatika

Program Pasca Sarjana

Universitas Atma Jaya Yogyakarta

2012

	Program Studi Magister Teknik Informatika Universitas Atma Jaya Yogyakarta	Nomor Dokumen	Halaman
		SKPL-SteganoCSS	1/21
	Revisi		

DAFTAR PERUBAHAN

Revisi	Deskripsi
A	
B	
C	
D	
E	
F	

INDEX TGL	-	A	C	D	E	F	G
Ditulis oleh							
Diperiksa oleh							
Disetujui oleh							

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	2/ 20
<p>Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika</p>		

Daftar Halaman Perubahan

Halaman	Revisi	Halaman	Revisi

Daftar Isi

1	Pendahuluan	7
1.1	Tujuan	7
1.2	Lingkup Masalah	7
1.3	Definisi, Akronim dan Singkatan	7
1.4	Referensi	8
1.5	Deskripsi umum (Overview)	8
2	Deskripsi Kebutuhan	9
2.1	Perspektif produk	9
2.2	Fungsi Produk	9
2.3	Karakteristik Pengguna	11
2.4	Batasan-batasan	11
2.5	Asumsi dan Ketergantungan	12
3	Kebutuhan khusus	12
3.1	Kebutuhan antarmuka eksternal	12
3.1.1	Antarmuka pemakai	12
3.1.2	Antarmuka perangkat keras	12
3.1.3	Antarmuka perangkat lunak	13
3.1.4	Antarmuka Komunikasi	13
3.2	Kebutuhan fungsionalitas Perangkat Lunak	13
3.2.1	Aliran Informasi	13
3.2.1.1	DFD Level 0	13
3.2.1.1.1	Entitas Data	13
3.2.1.1.2	Proses	13
3.2.1.1.3	Topologi	14
3.2.1.2	DFD Level 1	14
3.2.1.2.1	Entitas Data	14
3.2.1.2.2	Proses	14
3.2.1.2.3	Topologi	15
3.2.1.3	DFD Level 2 Sistem Penerima	15
3.2.1.3.1	Entitas Data	15
3.2.1.3.2	Proses	15

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	4/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

3.2.1.3.3 Topologi	16
3.2.1.4 DFD Level 2 Sistem Pengirim	16
3.2.1.4.1 Entitas Data	16
3.2.1.4.2 Proses	17
3.2.1.4.3 Topologi	17
3.2.1.5 DFD Level 3 Proses Ekstraksi Pesan	18
3.2.1.5.1 Entitas Data	18
3.2.1.5.2 Proses	18
3.2.1.5.3 Topologi	19
4 Kamus Data	19

Daftar Gambar

Gambar 1. DFD Level 0	14
Gambar 2. DFD Level 1	15
Gambar 3. DFD Level 2 Sistem penerima	17
Gambar 4. DFD Level 2 Sistem Pengirim	18
Gambar 5. DFD Level 3 Sistem Ekstraksi	20

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	6/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

1 Pendahuluan

1.1 Tujuan

Dokumen Spesifikasi Kebutuhan Perangkat Lunak (SKPL) ini merupakan dokumen spesifikasi kebutuhan perangkat lunak SteganoCSS yang dipakai sebagai acuan dalam pembuatan perangkat lunak. Dokumen ini mendefinisikan beberapa kebutuhan yang harus tersedia agar perangkat lunak dapat dikembangkan. Perangkat lunak ini dibuat untuk pengguna *personal computer* yang diharapkan dapat melakukan proses steganografi pada berkas *Cascading Style Sheet* (CSS).

1.2 Lingkup Masalah

Perangkat lunak "SteganoCSS" ini diimplementasikan menggunakan bahasa pemrograman PHP, data yang dibutuhkan berupa berkas teks dengan ekstensi *.css. fungsi-fungsi yang terdapat dalam perangkat lunak ini antara lain : generate, embedding, extracting.

1.3 Definisi, Akronim dan Singkatan

Daftar definisi akronim dan singkatan :

Keyword/Phrase	Definisi
SKPL	Merupakan spesifikasi kebutuhan dari perangkat lunak yang akan dikembangkan.
SKPL-SteganoCSS-XXX	Kode yang merepresentasikan kebutuhan pada SteganoCSS dimana XXX merupakan nomor fungsi.
SteganoCSS	Sistem steganografi pada berkas Cascading Style Sheet (CSS)
CSS	Berkas Cascading Style Sheet
Cover teks	Media penutup dalam proses steganografi, dalam aplikasi ini coverteks berupa CSS

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	7/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

Stego teks	Cover teks yang telah disisipkan pesan, stegoteks berupa berkas CSS
Kunci Publik	Kunci yang digunakan untuk proses enkripsi.
Kunci Privat	Kunci yang digunakan untuk proses dekripsi.

1.4 Referensi

Referensi yang digunakan adalah:

1. Template SKPL-PKODKBS, Program Studi Teknik Informatika Universitas Atma Jaya Yogyakarta.
2. Manual PHP, www.php.net.

1.5 Deskripsi umum (Overview)

Secara umum dokumen SKPL ini terbagi atas 3 bagian utama.

1. Pendahuluan yang berisi tujuan pembuatan dokumen ini, lingkup masalah, definisi, akronim dan singkatan, referensi, serta deskripsi umum tentang dokumen SKPL ini.
2. Berisi penjelasan umum tentang perangkat lunak SiPPUM yang akan dikembangkan, mencakup perspektif produk yang akan dikembangkan, fungsi produk perangkat lunak, karakteristik pengguna, batasan dalam penggunaan perangkat lunak dan asumsi yang dipakai dalam pengembangan perangkat lunak.
3. Penjelasan secara lebih rinci tentang kebutuhan khusus perangkat lunak yang akan dikembangkan.

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	8/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

2 Deskripsi Kebutuhan

2.1 Perspektif produk

SteganoCSS merupakan perangkat lunak yang dikembangkan dengan bahasa pemrograman PHP menggunakan editor teks Notepad++. Perangkat lunak ini diharapkan dapat membantu pengguna dalam hal keamanan data sehingga kerahasiaan datanya dapat terjaga.

Data teks yang akan dikirimkan berasal dari teks yang di inputkan oleh pengguna melalui *keyboard*. Berkas penutup dalam hal ini berkas CSS yang digunakan, merupakan berkas CSS aplikasi yang tersimpan di server.

2.2 Fungsi Produk

Perangkat lunak SteganoCSS yang akan diimplementasikan ini memiliki beberapa fungsi yaitu:

1. Fungsi Pembangkitan Pasangan Kunci (SKPL-SteganoCSS-001)

Merupakan fungsi yang digunakan pengguna untuk membangkitkan pasangan kunci, tidak ada data yang diinputkan, fungsi berjalan dengan data yang di bangkitkan secara random. Hal ini dimaksudkan untuk menghindari kesalahan pemilihan bilangan p dan q . Fungsi Pembangkitan Pasangan Kunci meliputi beberapa fungsi-fungsi berikut, diantaranya :

a. Fungsi Generate (SKPL-SteganoCSS-001-01) merupakan fungsi yang dijalankan ketika pengguna menekan tombol "generate" pada halaman utama aplikasi.

b. Fungsi Regenerate (SKPL-SteganoCSS-001-02) merupakan fungsi yang dijalankan ketika pengguna menekan tombol "regenerate" pada halaman pembangkitan kunci. Fungsi ini berguna untuk membangkitkan ulang pasangan kunci.

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	9/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

- c. Fungsi Simpan Kunci Publik (SKPL-SteganoCSS-001-03) merupakan fungsi yang digunakan untuk menyimpan kunci publik pada lingkungan *server*.
 - d. Fungsi Simpan Kunci Privat (SKPL-SteganoCSS-001-04) merupakan fungsi yang digunakan untuk menyimpan kunci privat/rahasia pada lingkungan *client*/komputer lokal.
2. Fungsi *Embedding* (SKPL-SteganoCSS-002).
- Fungsi penyisipan pesan ke dalam berkas CSS. Data yang dimasukkan adalah pasangan kunci publik dan pesan yang akan dikirim. Fungsi *Embedding* mencakup:
- a. Fungsi Pengecekan Maksimum Karakter (SKPL-SteganoCSS-002-01) merupakan fungsi untuk memeriksa kapasitas maksimum karakter yang dapat ditampung oleh *covert*teks, dalam hal ini berkas CSS.
 - b. Fungsi Enkripsi (SKPL-SteganoCSS-002-02) merupakan fungsi untuk mengenkripsi pesan menggunakan algoritma kriptografi RSA sehingga dihasilkan *ciphert*teks.
 - c. Fungsi Encode (SKPL-SteganoCSS-002-03) merupakan fungsi untuk mengkonversi *ciphert*teks menjadi bit-bit biner dan mengubahnya sekali lagi menjadi karakter *whitespace*.
 - d. Fungsi Embed (SKPL-SteganoCSS-002-04) adalah fungsi yang digunakan untuk menanamkan pesan terenkripsi ke dalam berkas CSS, setelah sebelumnya mengalami proses pada fungsi Encode.
3. Fungsi *Extracting* (SKPL-SteganoCSS-003).
- Fungsi *Extracting* merupakan fungsi untuk mendapatkan kembali pesan yang ada di dalam berkas CSS.
- Fungsi *Extracting* mencakup:

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	10/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

- a. Fungsi Decode (SKPL-SteganoCSS-003-01) merupakan fungsi untuk mengkonversi karakter-karakter *whitespace* menjadi bit-bit biner dan mengubahnya menjadi bilangan bulat sehingga siap untuk didekripsi.
- b. Fungsi Ekstrak (SKPL-SteganoCSS-003-02) adalah fungsi yang digunakan untuk mengekstrak pesan terenkripsi yang tertanam pada berkas CSS, fungsi ini dijalankan sebelum fungsi Decode.
- c. Fungsi Dekripsi (SKPL-SteganoCSS-003-03) yang merupakan fungsi untuk mendekrip cipherteks menjadi pesan asli (plainteks). Fungsi ini berjalan setelah fungsi decode.

2.3 Karakteristik Pengguna

Karakteristik dari pengguna perangkat lunak SteganoCSS dibedakan menjadi dua, yaitu :

1. Pengirim (*Sender*), yaitu siapa saja yang menggunakan aplikasi ini untuk mengirim pesan. Pengguna ini hanya menggunakan satu fungsi yaitu fungsi *Embedding*.
2. Penerima (*Receiver*), yaitu siapa saja yang menggunakan aplikasi ini untuk menerima pesan. Pengguna ini menggunakan dua fungsi yaitu fungsi *Generate* dan fungsi *Extracting*.

2.4 Batasan-batasan

Batasan-batasan dalam pengembangan perangkat lunak SteganoCSS ini adalah :

1. Kebijakan Umum
Berpedoman pada tujuan dari pengembangan perangkat lunak SteganoCSS.
2. Keterbatasan perangkat keras

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	11/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

Mengingat tidak adanya layanan pihak ketiga yang menyediakan modul yang dibutuhkan untuk menjalankan perangkat lunak ini, maka perangkat lunak hanya bisa diimplementasikan pada lingkungan *localhost*.

2.5 Asumsi dan Ketergantungan

Asumsi yang digunakan dalam pengembangan perangkat lunak SteganoCSS yaitu :

- a. Pengguna dari aplikasi ini dibedakan menjadi dua, pengirim dan penerima, yang berbeda menjalankan fungsinya masing-masing.
- b. Perangkat lunak ini tergantung pada ketersediaan modul PHP GMP library untuk melakukan perhitungan nilai integer yang besar.
- c. Perangkat lunak ini hanya dapat dijalankan dengan bantuan browser internet.

3 Kebutuhan khusus

3.1 Kebutuhan antarmuka eksternal

Kebutuhan antar muka eksternal pada perangkat lunak SteganoCSS ini meliputi kebutuhan antarmuka pemakai, antarmuka perangkat keras, antarmuka perangkat lunak dan antarmuka komunikasi.

3.1.1 Antarmuka pemakai

Personal komputer dengan sistem operasi yang dapat menjalankan browser internet.

3.1.2 Antarmuka perangkat keras

Antarmuka perangkat keras yang digunakan dalam perangkat lunak SteganoCSS adalah:

1. Perangkat komputer dengan spesifikasi prosesor minimal 1,2 GHz.
2. RAM minimal 256 MB.

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	12/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

3. Monitor, Keyboard dan Mouse.

3.1.3 Antarmuka perangkat lunak

Perangkat lunak yang dibutuhkan untuk mengoperasikan perangkat lunak SteganoCSS adalah sebagai berikut :

1. Sistem Operasi Microsoft Windows
2. Browser Internet
3. PHP Webserver
4. Notepad ++ sebagai editor penulisan kode program.

3.1.4 Antarmuka Komunikasi

Antarmuka komunikasi perangkat lunak SteganoCSS menggunakan protokol HTTP.

3.2 Kebutuhan fungsionalitas Perangkat Lunak

3.2.1 Aliran Informasi

Aliran informasi pada perangkat lunak ini akan ditunjukkan melalui DFD level 0, DFD level 1, DFD level 2, hingga DFD level 3.

3.2.1.1 DFD Level 0

3.2.1.1.1 Entitas Data

Pada DFD Level 0, yang ditunjukkan pada Gambar 1, terdapat satu entitas yaitu pengguna

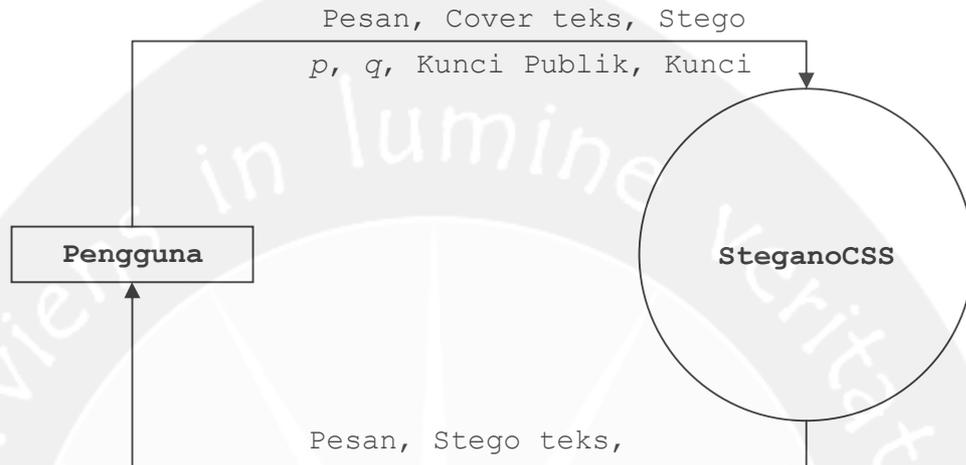
3.2.1.1.2 Proses

Pada level ini hanya ada satu entitas yaitu dari pengguna. Data dari pengguna menuju sistem adalah yang diperoleh dari piranti input (*keyboard*) dan cover teks yang diperoleh dari piranti penyimpanan. Pesan adalah teks yang berupa karakter-karakter ASCII. Cover teks adalah berkas dengan format *Cascading Style Sheet* (CSS) yang digunakan sebagai media untuk menyembunyikan pesan sehingga diperoleh stego teks dengan format yang sama yaitu CSS. Kunci Publik

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	13/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

dan Kunci Privat merupakan barisan bilangan bulat yang digunakan sebagai kunci enkripsi maupun dekripsi.

3.2.1.1.3 Topologi



Gambar 1. DFD Level 0

3.2.1.2 DFD Level 1

3.2.1.2.1 Entitas Data

Gambar 2 menunjukkan DFD Level 1, terdapat satu entitas data yang terlibat yaitu pengguna.

3.2.1.2.2 Proses

DFD Level 1 merupakan gambaran lebih detail yang ada pada DFD Level 0. Pada level ini DFD dibagi menjadi dua proses, yaitu:

1 Sistem Penerima

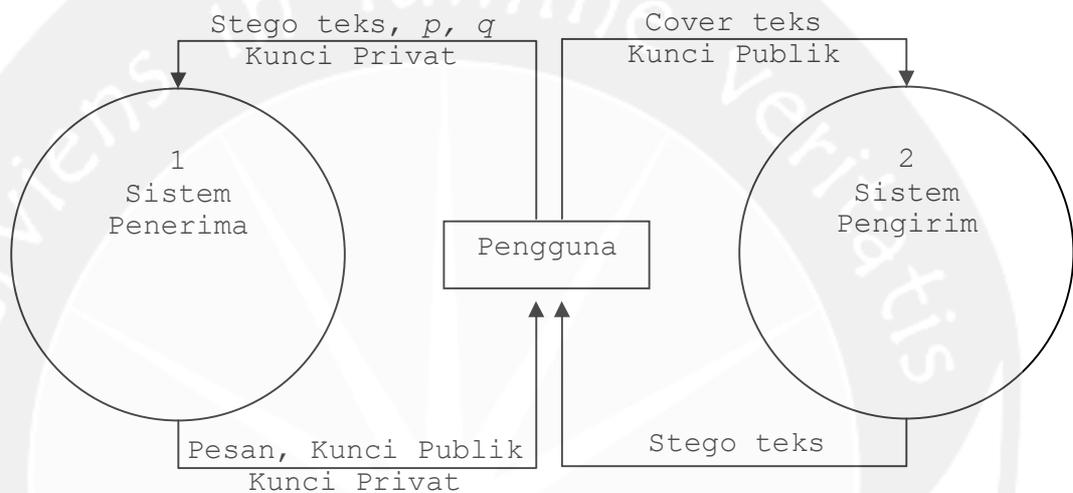
Sistem Penerima, memerlukan masukan (input) berupa nilai p , nilai q , stego teks dan kunci privat. Nilai p dan q digunakan untuk membangkitkan pasangan kunci, yaitu kunci publik dan kunci privat. Sistem ini juga menerima masukan stego teks dan kunci privat yang menghasilkan pesan asli.

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	14/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

2 Sistem Pengirim

Sistem Pengirim memerlukan masukan data berupa kunci publik dan cover teks. Proses penyisipan dan enkripsi berjalan pada sistem pengirim ini, sehingga nantinya keluaran yang dihasilkan berupa stego teks.

3.2.1.2.3 Topologi



Gambar 2. DFD Level 1

3.2.1.3 DFD Level 2 Sistem Penerima

3.2.1.3.1 Entitas Data

Pada DFD Level 2 Sistem Penerima (Gambar 3) hanya terdapat satu entitas yaitu pengguna.

3.2.1.3.2 Proses

Pada DFD level 2 untuk sistem penerima ditunjukkan pada Gambar 3. Terdapat 2 buah proses yaitu :

1.1 Proses Pembangkitan Kunci

Proses ini berfungsi untuk mendapatkan pasangan kunci publik dan kunci privat, kunci publik akan dikirimkan kepada sistem pengirim sedangkan kunci privat digunakan sendiri untuk proses ekstraksi. Masukan pada proses ini berupa nilai p dan q ,

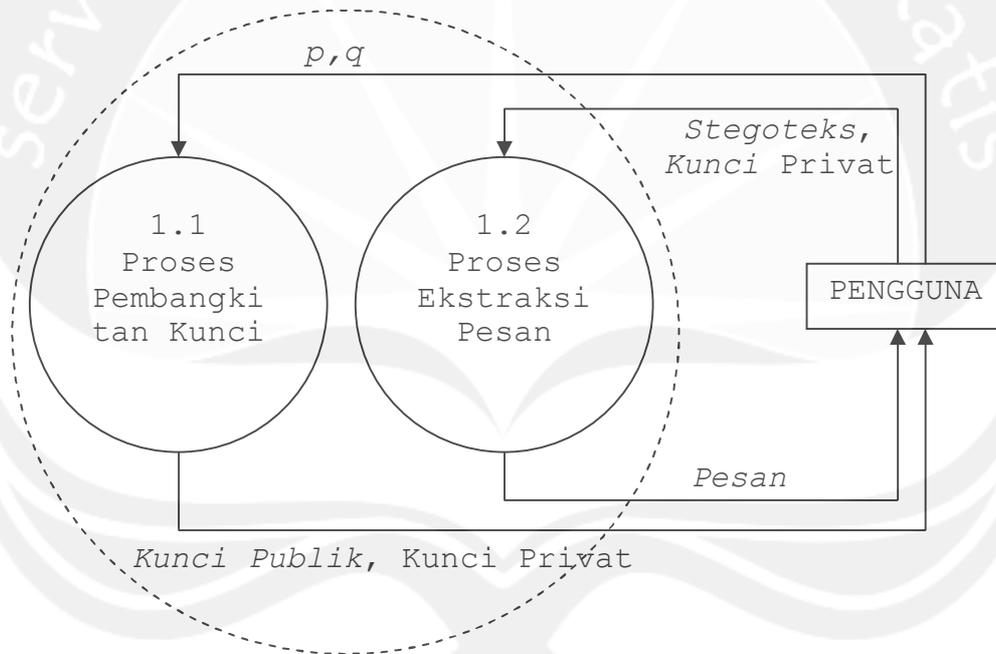
Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	15/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

yang menghasilkan keluaran berupa pasangan kunci publik dan kunci privat.

1.2 Proses Ekstraksi Pesan.

proses 1.2 adalah proses ekstraksi pesan, menggunakan kunci privat yang sebelumnya didapatkan pada proses 1.1 sebagai masukan data bersamaan dengan stego teks. Sehingga akhirnya keluaran dari proses 1.2 adalah berupa pesan asli.

3.2.1.3.3 Topologi



Gambar 3. DFD Level 2 Sistem Penerima

3.2.1.4 DFD Level 2 Sistem Pengirim

3.2.1.4.1 Entitas Data

Pada Gambar 4, menunjukkan entitas data yang terlibat pada level ini hanya satu yaitu pengguna.

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	16/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

3.2.1.4.2 Proses

DFD level 2 sistem pengirim merupakan diagram yang diuraikan secara lebih spesifik dari Proses 2 DFD level 1. DFD Level 2 Sistem Pengirim terdiri dari 3 proses, yaitu :

2.1 Proses Enkripsi

Proses enkripsi bekerja dengan masukan berupa teks pesan dan kunci publik. Keluaran dari proses 2.1 lalu digunakan sebagai masukan untuk proses 2.2.

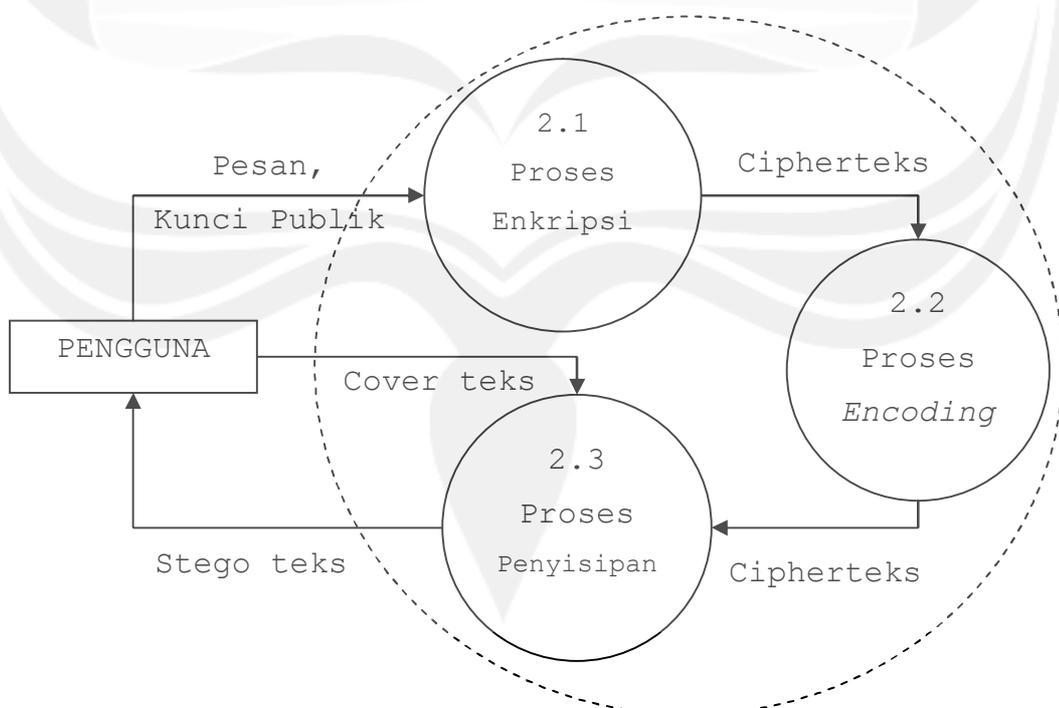
2.2 Proses encoding

Proses ini akan merubah cipherteks yang berupa bilangan desimal menjadi karakter whitespace.

2.3 Proses Penyisipan

Proses ini merupakan proses penyisipan cipherteks kedalam cover teks sehingga menghasilkan stego teks sebagai keluarannya.

3.2.1.4.3 Topologi



Gambar 4. DFD Level 2 Sistem Pengirim

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	17/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

3.2.1.5 DFD Level 3 Proses Ekstraksi Pesan

3.2.1.5.1 Entitas Data

DFD pada Level ini hanya melibatkan satu entitas data yaitu pengguna. DFD ditunjukkan pada gambar 5.

3.2.1.5.2 Proses

DFD level 3 untuk Proses Ekstraksi Pesan terdiri dari tiga proses, yaitu :

1.2.1 Proses Pengekstrakan

Proses ini adalah yang pertama dijalankan, dengan menggunakan masukan data berupa stego teks yang keluarannya digunakan pada proses 1.2.2.

1.2.2 Proses Decoding

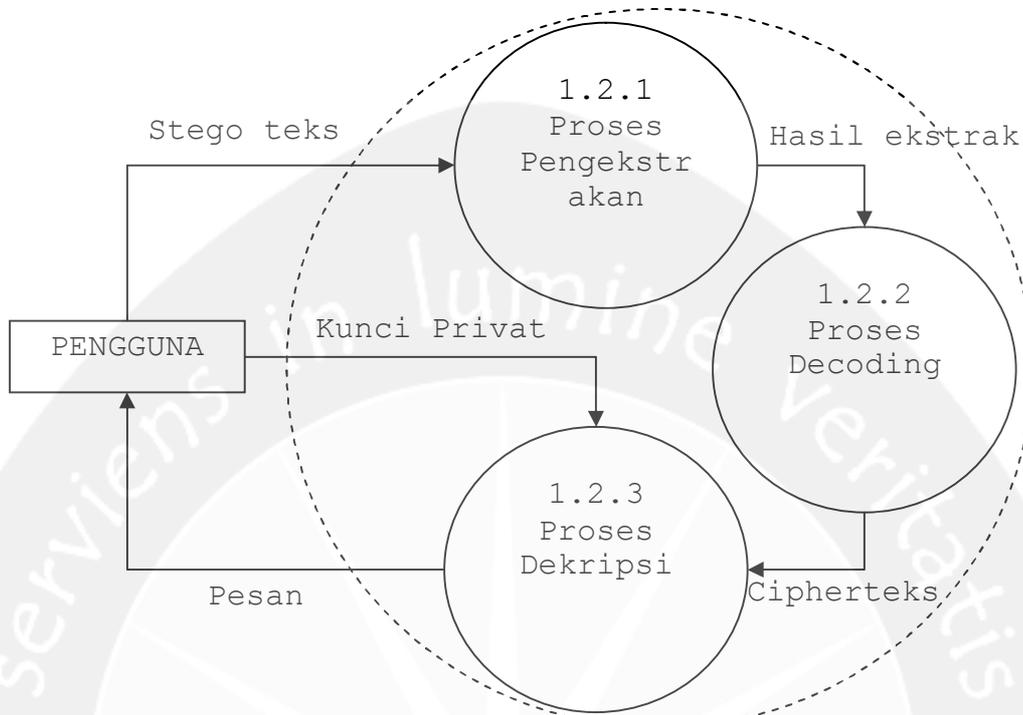
Proses ini berfungsi untuk merubah hasil ekstraksi yang masih berupa karakter-karakter *whitespace*, sehingga nantinya didapatkan cipherteks berupa bilangan bulat desimal yang siap untuk di dekripsi.

1.2.3 Proses Dekripsi

Merupakan proses dekripsi menggunakan algoritma RSA dengan masukan berupa cipherteks dari proses decoding dan kunci privat.

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	18/ 20
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

3.2.1.5.3 Topologi



Gambar 5. DFD Level 3 Proses Ekstraksi Pesan

4 Kamus Data

Elemen Data	Representasi	Domain	Range	Format	Presisi	Struktur Data
URL	Alamat cover teks yang berupa berkas CSS	text	-	CSS	-	varchar
KEY	Kunci Publik maupun Kunci Privat yang diperlukan untuk menyisipkan atau	number	-	pb, pv	-	number

Program Studi Magister Teknik Informatika	SKPL – SteganoCSS	19/ 20
--	-------------------	--------

Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika

	mengekstrak pesan					
Pesan	Pesan berupa teks karakter ASCII	text	-	-	-	varchar



DPPL

DESKRIPSI PERANCANGAN PERANGKAT LUNAK

SteganoCSS

Untuk : Tugas Akhir

Disusun oleh:

Herman Kabetta (105301476/PS/MTF)

Program Studi Magister Teknik Informatika

Program Pasca Sarjana

Universitas Atma Jaya Yogyakarta

2012

	Program Studi Magister Teknik Informatika Universitas Atma Jaya Yogyakarta	Nomor Dokumen		Halaman
		DPPL-SteganoCSS		1/13
		Revisi		

DAFTAR PERUBAHAN

Revisi	Deskripsi
A	
B	
C	
D	
E	
F	

INDEX TGL	-	A	C	D	E	F	G
Ditulis oleh							
Diperiksa oleh							
Disetujui oleh							

Program Studi Magister Teknik Informatika	DPPL – SteganoCSS	2/ 13
<p>Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika</p>		

Daftar Halaman Perubahan

Halaman	Revisi	Halaman	Revisi

Daftar Isi

1	Pendahuluan	6
1.1	Tujuan	6
1.2	Ruang Lingkup	6
1.3	Definisi dan Akronim	6
1.4	Referensi	7
1.5	Deskripsi Umum Dokumen	7
2	Deskripsi Arsitektural.....	8
3	Deskripsi Antarmuka dan Prosedural.....	8
3.1	Halaman Utama	8
3.2	Halaman Pembangkit Pasangan Kunci	9
3.3	Halaman Embedding	11
3.4	Halaman Extracting	12

Program Studi Magister Teknik Informatika	DPPL – SteganoCSS	4/ 13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

Daftar Gambar

1. Arsitektural Perangkat Lunak.....8
2. Halaman Utama.....8
3. Halaman Pembangkit Pasangan Kunci.....9
4. Halaman Proses Embedding.....11
5. Halaman Proses Extracting.....12



1 Pendahuluan

Dokumen Deskripsi Perancangan Perangkat Lunak (DPPL) bertujuan untuk mendefinisikan perancangan perangkat lunak "SteganoCSS" sebagai alat bantu untuk penelitian dengan judul "Skema Keamanan Steganografi Pada Cascading Style Sheet Menggunakan Sistem Kriptografi Kunci Publik". Dokumen DPPL ini digunakan oleh pengembang perangkat lunak sebagai acuan untuk implementasi pada tahap selanjutnya.

1.1 Tujuan

Perangkat lunak SteganoCSS ini dikembangkan dengan tujuan untuk dapat melakukan proses penyisipan pesan ke dalam berkas CSS (Cascading Style Sheet) yang dienkripsi menggunakan algoritma kunci publik RSA.

1.2 Ruang Lingkup

Perangkat lunak SteganoCSS ini berjalan pada lingkungan web dengan platform Windows, yang diimplementasikan menggunakan bahasa pemrograman PHP. Hasil akhir dari proses ini akan disimpan dalam berkas berformat CSS (*.CSS).

1.3 Definisi dan Akronim

Daftar definisi akronim dan singkatan :

Keyword/Phrase	Definisi
DPPL	Deskripsi Perancangan Perangkat Lunak atau disebut juga Software Design Description (SDD) merupakan deskripsi dari perancangan produk/perangkat lunak yang akan dikembangkan.
SteganoCSS	Perangkat lunak steganografi pada berkas CSS.
Cover teks	Media penutup dalam proses steganografi, dalam aplikasi ini covertteks berupa CSS

Stego teks	Cover teks yang telah disisipkan pesan, stegoteks berupa berkas CSS
Kunci Publik	Kunci yang digunakan untuk proses enkripsi.
Kunci Privat	Kunci yang digunakan untuk proses dekripsi.

1.4 Referensi

Referensi yang digunakan pada perangkat lunak tersebut adalah:

1. Template DPPL-PKODKBS, Program Studi Teknik Informatika Universitas Atma jaya Yogyakarta.
2. Gahara Rafael Anggara Wira, Pengaruh Steganografi Terhadap Resolusi Warna Dalam File Citra Format Joint Photographic Expert Group (JPEG).
3. Manual PHP, www.php.net.

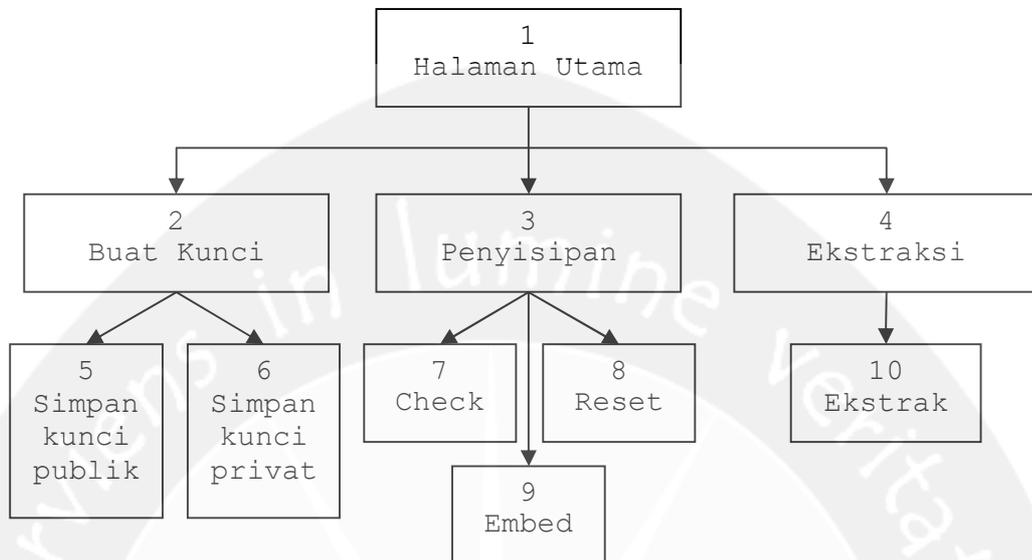
1.5 Deskripsi Umum Dokumen

Dokumen DPPL ini dibagi menjadi empat bagian yaitu :

1. Pendahuluan, berisi tujuan pembuatan dokumen ini, lingkup masalah, definisi, akronim dan singkatan serta deskripsi umum.
2. Deskripsi arsitektural
3. Deskripsi antarmuka dan prosedural berisi gambaran halaman-halaman yang akan digunakan beserta tombol-tombol dan fitur yang ada pada form tersebut.
4. Deskripsi data yang berisi penjelasan tentang tabel-tabel yang digunakan dalam perangkat lunak ini.

Program Studi Magister Teknik Informatika	DPPL – SteganoCSS	7/ 13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

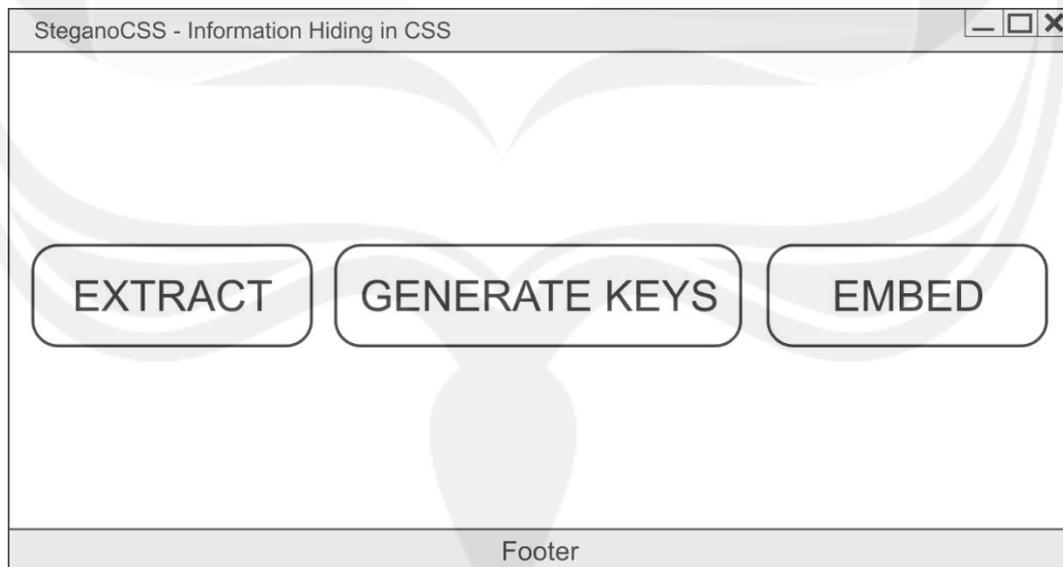
2 Deskripsi Arsitektural



Gambar 1 Arsitektural Perangkat Lunak

3 Deskripsi Antarmuka dan Prosedural

3.1 Halaman Utama



Gambar 2 Halaman Utama

a. Generate Button Click

Kamus Data	- Rand p, rand q : random integer
Algoritma	<pre> Input : - Output : publicKey, privateKey n ← rand_p * rand_q totient ← (rand_p-1)*(rand_q-1) for e = 2 to e = 99 if gcd(e,totient) = 1 then break end if end for i ← 1 do d ← ((totient*i)+1)/e i + 1 while (d*e) mod(totient)=1 </pre>

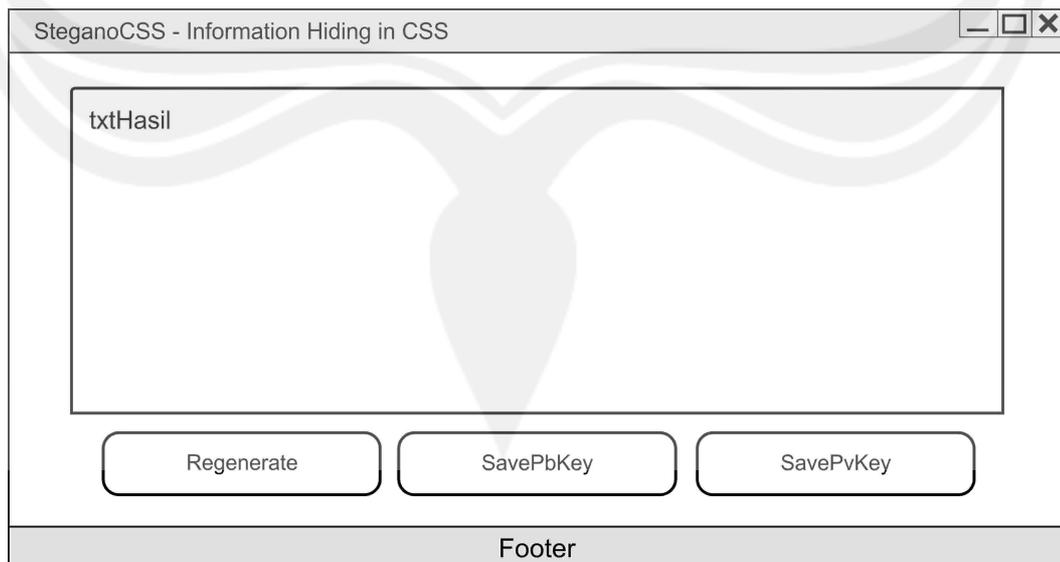
b. Embed Button Click

Kamus Data	-
Algoritma	<pre> Input : - Output : Goto embedding page </pre>

c. Extract Button Click

Kamus Data	-
Algoritma	<pre> Input : - Output : Goto extracting page </pre>

3.2 Halaman Pembangkit Pasangan Kunci



Gambar 3 Halaman Pembangkit Pasangan Kunci

Program Studi Magister Teknik Informatika	DPPL – SteganoCSS	9/ 13
<p>Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika</p>		

a. Regenerate Button Click

Kamus Data	- Rand_p, rand_q : random integer. - txtHasil : text
Algoritma	<pre> Input : - Output : publicKey, privateKey n ← rand_p * rand_q totient ← (rand_p-1)*(rand_q-1) for e = 2 to e = 99 if gcd(e,totient) = 1 then break end if end for i ← 1 do d ← ((totient*i)+1)/e i + 1 while (d*e) mod(totient)≠1 </pre>

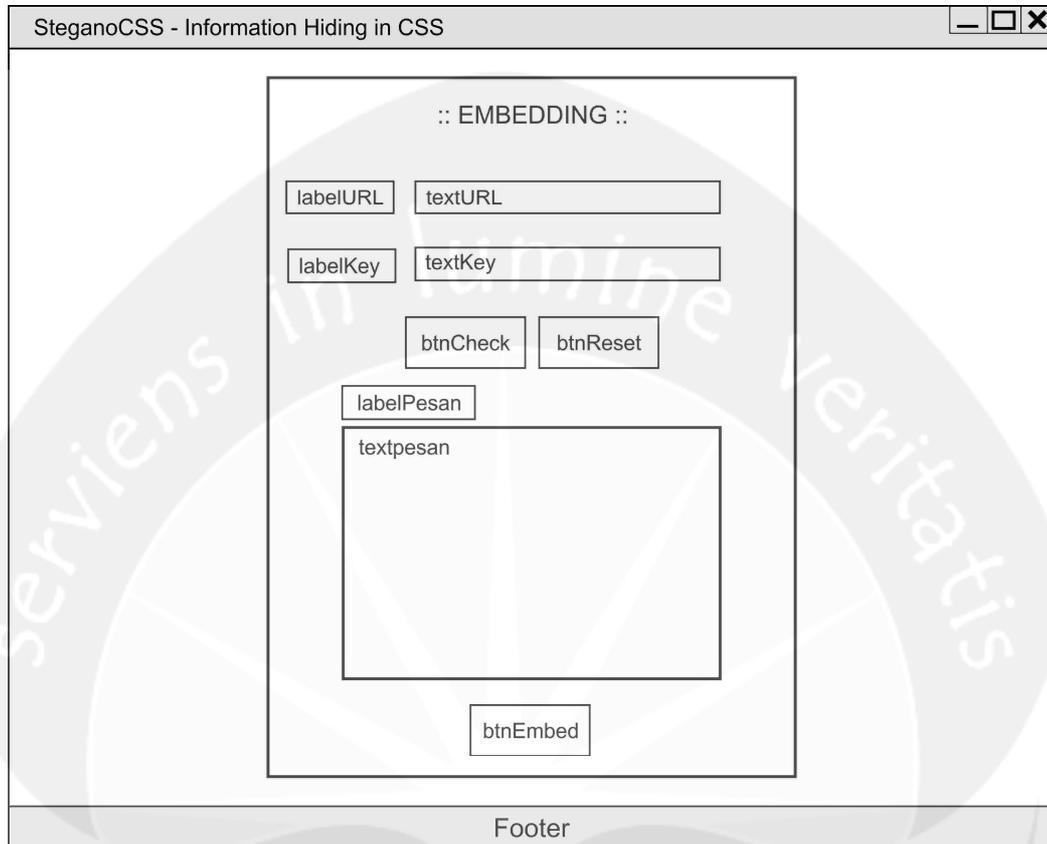
b. SavePbKey Button Click

Kamus Data	- Key.pb : textFile
Algoritma	<pre> Input : - Output : key.pb </pre>

c. SavePvKey Button Click

Kamus Data	- Key.pv : textFile
Algoritma	<pre> Input : - Output : key.pv </pre>

3.3 Halaman Embedding



Gambar 4 Halaman Proses Embedding

a. BtnCheck Click

Kamus Data	- textURL : text, textKey : text
Algoritma	<pre> Input : textURL, textKey[e,n] Output : maxChar Read per Row of textURL If find char(";") on EndOfLine Then count++ Else If null End If maxChar = (floor(count/(4*(n+1))))*10 </pre>

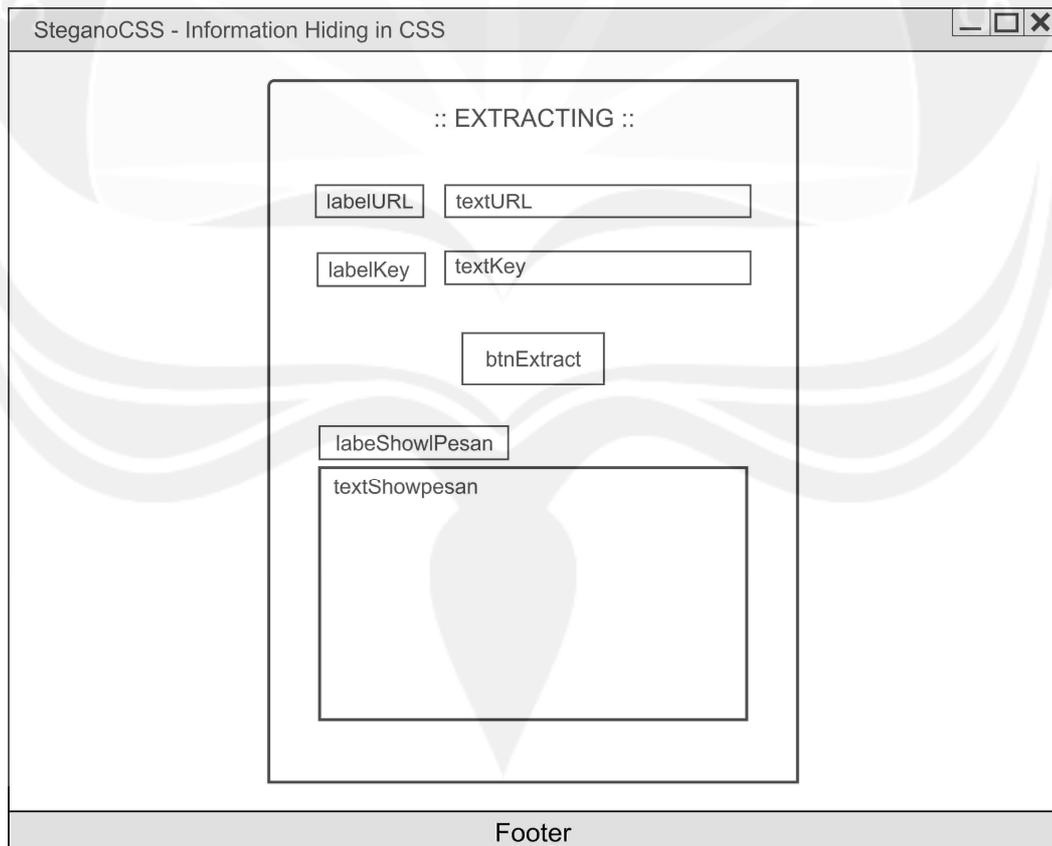
b. btnReset Click

Kamus Data	-
Algoritma	<pre> Input : - Output : - Clear all text </pre>

c. btnEmbed Click

Kamus Data	- textURL : text, textKey : text - textPesanan : text
Algoritma	Input : textURL, textKey[e,n], textPesanan Output : style.css textAsc = ConvertToASCII(textPesanan) Encoded =R SAencrypt(textAsc,e,n) EncBin = ConvertToBinary(Encoded) EncWhi = ConvertToWhitespace(EncBin) Read per Row of textURL Clear All Whitespace on EndOfLine If find char(";") on EndOfLine Then Print EncWhi on EndOfLine Else If Print null on EndOfLine End If

3.4 Halaman Extracting



Gambar 5 Halaman Proses Extracting

Program Studi Magister Teknik Informatika	DPPL – SteganoCSS	12/ 13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

a. btnExtract Click

Kamus Data	<ul style="list-style-type: none"> - textURL : text, textKey : text - textShowPesan : text
Algoritma	<pre> Input : textURL, textKey[d,n] Output : textShowPesan EncWhi = null Read per Row of textURL If find Whitespace on EndOfLine Then EncWhi = EncWhi + Whitespace End If EncBin = ConvertToBinary(EncWhi) textAsc = ConvertToASCII(EncBin) textShowPesan = RSAdecrypt(TextAsc,d,n) Print textShowPesan </pre>



PDHUPL

PERENCANAAN, DESKRIPSI, DAN HASIL UJI
PERANGKAT LUNAK

SteganoCSS

Untuk : Tugas Akhir

Disusun oleh:

Herman Kabetta (105301476/PS/MTF)

Program Studi Magister Teknik Informatika

Program Pasca Sarjana

Universitas Atma Jaya Yogyakarta

2012

	Program Studi Magister Teknik Informatika Universitas Atma Jaya Yogyakarta	Nomor Dokumen		Halaman
		PDHUPL-SteganoCSS		1/13
		Revisi		

DAFTAR PERUBAHAN

Revisi	Deskripsi
A	
B	
C	
D	
E	
F	

INDEX TGL	-	A	C	D	E	F	G
Ditulis oleh							
Diperiksa oleh							
Disetujui oleh							

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	2/ 13
--	---------------------	-------

Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika

Daftar Halaman Perubahan

Halaman	Revisi	Halaman	Revisi

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	3/ 13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

Daftar Isi

1	Pendahuluan.....	5
1.1	Tujuan	5
1.2	Definisi, Akronim dan Singkatan	5
1.3	Referensi	6
1.4	Deskripsi umum (Overview)	6
2	Lingkungan Pengujian Perangkat Lunak	7
2.1	Perangkat Lunak Pengujian	7
2.2	Perangkat Keras Pengujian	7
2.3	Material Pengujian	7
2.4	Sumber Daya Manusia	7
2.5	Prosedur Umum Pengujian	8
3	Identifikasi dan Rencana Pengujian	9
4	Deskripsi dan Hasil Uji	11

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	4/ 13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

1 Pendahuluan

1.1 Tujuan

Dokumen Perencanaan, Deskripsi dan Hasil Uji Perangkat Lunak (PDHUPL) ini digunakan sebagai bahan panduan untuk melakukan pengujian terhadap perangkat lunak "SteganoCSS" sebagai alat bantu untuk penelitian dengan judul "Skema Keamanan Steganografi Pada Cascading Style Sheet Menggunakan Sistem Kriptografi Kunci Publik". Dokumen PDHUPL ini digunakan oleh pengembang perangkat lunak untuk menguji keseluruhan aplikasi SteganoCSS.

1.2 Definisi, Akronim dan Singkatan

Tabel 1. Daftar definisi akronim dan singkatan

Keyword/Phrase	Definisi
PDHUPL	Merupakan Dokumen Perencanaan, Deskripsi dan Hasil Uji Perangkat Lunak yang dibuat.
PDHUPL- SteganoCSS-XXX	Kode yang merepresentasikan kebutuhan pada Sistem SteganoCSS dimana XXX merupakan nomor fungsi produk.
SteganoCSS	Perangkat lunak untuk menanamkan pesan rahasia pada berkas <i>Cascading Style Sheet</i> .
CSS	Singkatan dari <i>Cascading Style Sheet</i> yang merupakan berkas untuk mengatur tampilan situs web.
Internet	Internet merupakan istilah umum yang dipakai untuk menunjuk <i>Network</i> global yang terdiri dari komputer dan layanan servis dengan sekitar 30 sampai 50 juta pemakai komputer dan puluhan layanan informasi termasuk e-mail, FTP, dan World Wide Web.
Server	Komputer yang menyediakan sumber daya bagi klien yang terhubung melalui jaringan.

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	5/13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

Program	Data yang berisikan daftar program baik hasil penelitian maupun kreativitas.
User	Pengguna sistem

1.3 Referensi

Referensi yang digunakan pada perangkat lunak tersebut adalah:

1. Template PDHUPL, Program Studi Teknik Informatika Universitas Atma jaya Yogyakarta.
2. Manual PHP, www.php.net.

1.4 Deskripsi umum (Overview)

Secara umum dokumen PDHUPL ini terbagi atas 4 bagian utama. Bagian pertama berisi penjelasan mengenai dokumen PDHUPL tersebut yang mencakup tujuan pembuatan PDHUPL, definisi, akronim dan singkatan-singkatan yang digunakan dalam pembuatan PDHUPL, referensi dan deskripsi umum tentang dokumen PDHUPL ini.

Bagian kedua berisi penjelasan mengenai lingkungan pengujian perangkat lunak yang mencakup perangkat lunak dan perangkat keras pengujian, material pengujian, sumber daya manusia dan prosedur umum pengujian.

Bagian ketiga berisi pengidentifikasian dan perencanaan pengujian terhadap perangkat lunak yang telah dibuat. Sedangkan bagian keempat berisi penjelasan/ deskripsi dan laporan hasil uji fungsionalitas perangkat lunak.

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	6/13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

2 Lingkungan Pengujian Perangkat Lunak

2.1 Perangkat Lunak Pengujian

Perangkat lunak Pengujian berupa:

1. Windows 7 Ultimate 64-Bit dari Microsoft sebagai sistem operasi.
2. PHP sebagai bahasa pemrograman yang digunakan untuk membangun perangkat lunak.
3. HTML dan Javascript sebagai bahasa pemrograman pendukung untuk membangun perangkat lunak.
4. Notepad++ sebagai antarmuka penulisan kode perangkat lunak.
5. Apache sebagai web server dengan ekstensi php_gmp aktif.
6. Mozilla Firefox sebagai web browser.

2.2 Perangkat Keras Pengujian

Laptop dengan spesifikasi Processor AMD Turion(tm) II Dual-Core Mobile M500 2.20 GHz dan RAM 2 GB.

2.3 Material Pengujian

Material tambahan yang dibutuhkan dalam pengujian adalah sebagai berikut:

1. Listing kode PHP program SteganoCSS.
2. Berkas Style.CSS sebagai berkas penutup/covertteks.

2.4 Sumber Daya Manusia

Sumber daya manusia yang terlibat dalam kegiatan pengujian perangkat lunak SteganoCSS berjumlah 1 orang dengan tingkat keahlian dan kriteria sebagai berikut :

1. Memiliki pemahaman tentang metode dan teknik pengujian perangkat lunak yang benar.
2. Memiliki kemampuan untuk mencari kesalahan yang terdapat pada perangkat lunak dan cara penanganan untuk memperbaikinya.

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	7/13
--	---------------------	------

Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika

3. Memahami cara kerja perangkat lunak SteganoCSS.
4. Memahami mengenai materi kriptografi khususnya algoritma kunci publik RSA.
5. Memahami mengenai sistem steganografi khususnya metode *end of line*.

2.5 Prosedur Umum Pengujian

2.5.1 Pengenalan dan Latihan

Pada pengujian perangkat lunak ini tidak dilakukan pengenalan maupun pelatihan terhadap perangkat lunak SteganoCSS, dengan asumsi bahwa penguji telah memiliki pengetahuan tentang Kriptografi dan Steganografi.

2.5.2 Persiapan Awal

2.5.2.1 Persiapan Prosedural

Pengujian dilakukan di kampus 3 Universitas Atma Jaya Yogyakarta dengan menginstal Perangkat Lunak yang dibutuhkan untuk mendukung perangkat lunak yang telah dibuat.

2.5.2.2 Persiapan Perangkat Keras

Pada persiapan perangkat keras dilakukan pengecekan terhadap komputer jinjing yang dipakai.

2.5.2.3 Persiapan Perangkat Lunak

1. Instalasi perangkat lunak SteganoCSS.
2. Menyiapkan skenario pengujian untuk memeriksa kebenaran program.

2.5.3 Pelaksanaan

Pelaksanaan pengujian dilaksanakan dalam satu tahap, yaitu pengujian terhadap terhadap aplikasi web. Strategi pengujian yang dilakukan ialah pengujian secara totalitas dengan melihat fungsional yang diberikan oleh perangkat lunak. Pengujian didasarkan pada kebutuhan yang harus dipenuhi oleh aplikasi SteganoCSS. Dengan demikian, pengujian tidak

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	8/13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

didasarkan pada modularitas aplikasi tetapi lebih didasarkan pada kebenaran fungsionalitas yang harusnya dicapai. Tingkat pengujian dibagi menjadi pengujian sistem dan pengujian unit. Pengujian tidak dilakukan pada lingkungan operasional yang sesungguhnya, tetapi pada salah satu komputer yang dimiliki oleh developer program.

2.5.4 Pelaporan Hasil

Hasil pengujian akan diserahkan kepada Dosen Pembimbing Penelitian.

3 Identifikasi dan Rencana Pengujian

Tabel 2. Identifikasi Pengujian

Kelas Uji	Butir Uji	Identifikasi		Jenis Uji	Jadwal
		SKPL	PDHUPL		
Performansi	Waktu Tanggap	SKPL- STEGANOCSS- 001,002,003	PDHUPL- STEGANOCSS- 001	Blackbox	05/09/12
Antarmuka pengguna	Pengujian Antarmuka Hasil Pembangkitan Kunci	SKPL- STEGANOCSS- 001	PDHUPL- STEGANOCSS- 002	Blackbox	05/09/12
	Pengujian Antarmuka Proses Embedding	SKPL- STEGANOCSS- 002	PDHUPL- STEGANOCSS- 003	Blackbox	05/09/12
	Pengujian Antarmuka Proses Extracting	SKPL- STEGANOCSS- 003	PDHUPL- STEGANOCSS- 004	Blackbox	05/09/12
Proses Pembangkitan Kunci	Pengujian Proses Pembangkitan Kunci	SKPL- STEGANOCSS- 001	PDHUPL- STEGANOCSS- 005	Blackbox	05/09/12
	Pengujian Proses Regenerate	SKPL- STEGANOCSS- 001	PDHUPL- STEGANOCSS- 005	Blackbox	05/09/12
	Pengujian Proses menyimpan pasangan Kunci	SKPL- STEGANOCSS- 001	PDHUPL- STEGANOCSS- 005	Blackbox	05/09/12

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	9/13
--	---------------------	------

Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika

Proses Embedding	Pengujian Maximum Characters Check	SKPL- STEGANOCSS- 002	PDHUPL- STEGANOCSS- 006	Blackbox	05/09/12
	Pengujian Proses Enkripsi	SKPL- STEGANOCSS- 002	PDHUPL- STEGANOCSS- 006	Blackbox	05/09/12
	Pengujian Proses Encoding	SKPL- STEGANOCSS- 002	PDHUPL- STEGANOCSS- 006	Blackbox	05/09/12
	Pengujian Proses Embedding	SKPL- STEGANOCSS- 002	PDHUPL- STEGANOCSS- 006	Blackbox	05/09/12
Proses Extracting	Pengujian Proses Extracting	SKPL- STEGANOCSS- 003	PDHUPL- STEGANOCSS- 007	Blackbox	05/09/12
	Pengujian Proses Decoding	SKPL- STEGANOCSS- 003	PDHUPL- STEGANOCSS- 007	Blackbox	05/09/12
	Pengujian Proses Dekripsi	SKPL- STEGANOCSS- 003	PDHUPL- STEGANOCSS- 007	Blackbox	05/09/12

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	10/ 13
--	---------------------	--------

Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika

4 Deskripsi dan Hasil Uji

Tabel 3. Deskripsi dan Hasil Pengujian

Identifikasi	Deskripsi	Prosedur Pengujian	Masukan	Keluaran yg diharapkan	Kriteria Evaluasi Hasil	Hasil yang Didapat	Kesimpulan
PDHUPL-SteganoCSS-001	Pengguna menerima indikasi reaksi aplikasi SteganoCSS terhadap aksinya maksimal empat detik setelah aksi dilakukan.	Membuka halaman utama, serta proses-proses pada halaman lain perangkat lunak untuk kemudian dihitung berapa lama waktu tanggapnya.	Pasangan kunci, teks pesan, lokasi berkas CSS.	Sistem dapat menampilkan halaman-halaman yang dimaksud dalam waktu kurang dari empat detik.	Setiap masukan dari pengguna, sistem dapat diproses dan di respon dalam waktu kurang dari empat detik.	Sistem dapat menampilkan halaman-halaman yang dimaksud dalam waktu kurang dari dua detik.	Handal
PDHUPL-SteganoCSS-002	Pengujian Display Hasil dari Pembangkitan pasangan kunci, yaitu kunci publik dan kunci privat.	Pengujian dilakukan dengan memilih/menekan tombol "generate" pada halaman utama, sehingga hasil dari pembangkitan kunci ditampilkan pada halaman pembangkit kunci.	-	Masuk ke halaman pembangkit kunci, dan hasil pembangkitan yang ditampilkan dengan benar.	Memasuki halaman pembangkit kunci dan hasil dari pembangkitan kunci ditampilkan dengan benar.	Memasuki halaman pembangkit kunci dan hasil pembangkitan kunci ditampilkan dengan benar.	Handal
PDHUPL-SteganoCSS-003	Pengujian Display antarmuka proses <i>embedding</i> , dan kemudian menampilkan hasilnya.	Pengujian dilakukan dengan memilih/menekan tombol "embed" pada halaman utama.	URL, kunci publik, teks pesan.	Halaman proses <i>embedding</i> ditampilkan, dan berpindah ke halaman hasil setelah proses <i>embedding</i> dilakukan.	Halaman proses <i>embedding</i> ditampilkan, dan berpindah ke halaman hasil setelah proses <i>embedding</i> dilakukan.	Halaman proses <i>embedding</i> berhasil ditampilkan, dan kemudian berpindah ke halaman hasil setelah proses <i>embedding</i> dilakukan.	Handal

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	11/ 13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		

PDHUPL- SteganoCSS- 004	Pengujian Display antarmuka proses <i>extracting</i> , dan kemudian menampilkan hasilnya.	Pengujian dilakukan dengan memilih/menekan tombol "embed" pada halaman utama.	URL, kunci privat.	Halaman proses <i>extracting</i> ditampilkan.	Halaman proses <i>extracting</i> ditampilkan.	Halaman proses <i>extracting</i> berhasil ditampilkan.	Handal
PDHUPL SteganoCSS- 005	Pengujian proses Pembangkitan pasangan kunci, yaitu kunci publik dan kunci privat.	Pengujian dilakukan dengan memilih/menekan tombol "generate" pada halaman utama, dilanjutkan dengan membangkitkan ulang pasangan kunci dengan memilih/menekan tombol "regenerate" pada halaman pembangkit kunci. Pengujian kedua yaitu pada proses menyimpan pasangan kunci, dengan memilih/menekan tombol save.	-	Data-data mengenai variabel pembangkit kunci ditampilkan dengan benar sesuai dengan algoritma pembangkit kunci RSA, baik itu saat pertama membangkitkan maupun setelah membangkitkan ulang, dan pasangan kunci dapat di simpan.	Data-data mengenai variabel pembangkit kunci ditampilkan dengan benar sesuai dengan algoritma pembangkit kunci RSA, baik itu saat pertama membangkitkan maupun setelah membangkitkan ulang, dan pasangan kunci dapat di simpan.	Data-data mengenai variabel pembangkit kunci berhasil ditampilkan dengan benar sesuai dengan algoritma pembangkit kunci RSA, baik itu saat pertama membangkitkan maupun setelah membangkitkan ulang, dan pasangan kunci berhasil di simpan.	Handal
PDHUPL- SteganoCSS- 006	Pengujian proses <i>embedding</i> , meliputi maximum character check, enkripsi, encoding, dan proses	Pengujian dilakukan dengan memilih/menekan tombol "embed" pada halaman utama, dilanjutkan dengan menekan tombol "check" dan "reset" pada halaman proses <i>embedding</i> setelah	URL, kunci publik, teks pesan.	Sistem menampilkan notifikasi mengenai karakter maksimum yang dapat ditampung oleh berkas CSS, serta dapat mengulangi proses pengecekan	Jika kolom inputan pada halaman aplikasi masih kosong, maka pengguna tidak dapat melanjutkan ke proses selanjutnya, di	Sistem berhasil menampilkan notifikasi mengenai karakter maksimum yang dapat ditampung oleh berkas CSS, serta berhasil mengulangi proses pengecekan menggunakan tombol	Handal

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	12/ 13
<p>Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika</p>		

	<i>embedding</i> itu sendiri.	sebelumnya memasukkan URL berkas CSS dan kunci publik pada form inputan. Pengujian kedua dilakukan dengan menekan tombol "embed" pada halaman proses <i>embedding</i> setelah sebelumnya memasukkan pesan pada form inputan.		menggunakan tombol "reset". Setelah proses <i>embedding</i> dijalankan, hasil dari proses ini akan ditampilkan dan diharapkan pesan tidak terlihat pada berkas penutup, atau dapat dikatakan berkas stego identik dengan berkas asli.	beritahukan melalui notifikasi dari sistem.	"reset". Setelah proses <i>embedding</i> dijalankan, hasil dari proses ini berhasil ditampilkan dan pesan berhasil disembunyikan pada berkas penutup, atau dapat dikatakan berkas stego sangat identik dengan berkas asli.	
PDHUPL-SteganoCSS-007	Pengujian proses <i>extracting</i> , <i>decoding</i> , dekripsi dan proses <i>extracting</i> itu sendiri.	Pengujian dilakukan dengan memilih/menekan tombol "extract" pada halaman utama, dilanjutkan dengan menekan tombol "extract" pada halaman proses <i>extracting</i> setelah sebelumnya memasukkan URL dan kunci privat pada form inputan.	URL, Kunci Privat	Sistem menampilkan pesan rahasia sesuai dengan yang telah ditanamkan pada proses sebelumnya.	Jika kunci yang dimasukkan salah, maka pesan yang sebenarnya tidak akan ditampilkan dengan benar.	Sistem berhasil menampilkan pesan rahasia sesuai dengan yang telah ditanamkan pada proses sebelumnya menggunakan kunci yang benar. Sistem menampilkan pesan berbeda atau palsu jika menggunakan kunci yang salah.	Handal

Program Studi Magister Teknik Informatika	PDHUPL – SteganoCSS	13/ 13
Dokumen ini dan informasi yang dimilikinya adalah milik Program Studi Magister Teknik Informatika-UAJY dan bersifat rahasia. Dilarang untuk me-reproduksi dokumen ini tanpa diketahui oleh Program Studi Magister Teknik Informatika		