

**Prototipe Sistem Kriptografi Kunci Publik Algoritma Rivest
Shamir Adleman (RSA) Untuk Keamanan Pertukaran Data
Dengan Bahasa Pemrograman Java Server Pages (JSP)**

TESIS



Oleh:

**Fuad Lutfi
1111600282**

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2013**

**Prototipe Sistem Kriptografi Kunci Publik Algoritma Rivest
Shamir Adleman (RSA) Untuk Keamanan Pertukaran Data
Dengan Bahasa Pemrograman Java Server Pages (JSP)**

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (MKOM)



Oleh:

Fuad Lutfi

1111600282

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2013**



PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama Mahasiswa : Fuad Lutfi
Nomor Induk Mahasiswa : 1111600282
Program Studi : Magister Ilmu Komputer
Konsentrasi : Teknologi Sistem Informasi
Fakultas/Program : Pasca Sarjana

menyatakan bahwa Tesis yang berjudul:

Prototipe Sistem Kriptografi Kunci Publik Algoritma Rivest Shamir Adleman (RSA)
Untuk Keamanan Pertukaran Data Dengan Bahasa Pemrograman Java Server Pages (JSP)

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 22 Agustus 2013


Fuad Lutfi

METERAI
TEMPIL
PAJAK PEMANGKUTAN BANGSA
TGL. 20
D018DABF278147544
ENAM RIBU RUPIAH
6000 LJP



PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Fuad Lutfi
Nomor Induk Mahasiswa : 1111600282
Konsentrasi : Teknologi Sistem Informasi
Judul Tesis : Prototipe Sistem Kriptografi Kunci Publik Algoritma
Rivest Shamir Adleman (RSA) Untuk Keamanan
Pertukaran Data Dengan Bahasa Pemrograman Java
Server Pages (JSP)

Jakarta, 22 Agustus 2013

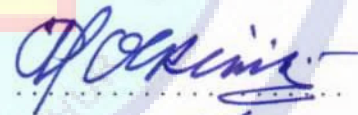
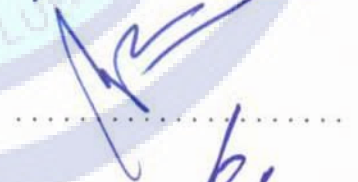
Tim Penguji:

Ketua,
Dr. Moedjiono, M.Sc

Anggota,
Dr. Ir Wendi Usino, M.Sc, MM

Pembimbing,
Dr. Ir. Nazori Az, M.T

Tanda Tangan:


.....

.....

.....

Ketua Program Studi


Dr., Ir. Nazori Az, M.T

ABSTRAK

Pesatnya perkembangan teknologi informasi menggunakan komputer, mengakibatkan semakin bertambah pula masalah yang mengiringi perkembangan teknologi tersebut. Masalah keamanan data merupakan faktor yang harus diperhatikan dalam perkembangan teknologi informasi selanjutnya. Jika membicarakan tentang teknologi informasi tentunya berkaitan pula dengan isi yang terkandung dalam informasi tersebut. Informasi yang akan disampaikan/dikirimkan haruslah sesuai dengan isi yang ingin diinformasikan. Pengiriman data dan informasi hendaknya dapat memastikan keamanan dari data dan informasi yang dikirimkannya, sehingga pengiriman informasi dapat dipertanggung jawabkan dari segi kerahasiaan data dan informasi, keaslian data dan informasinya, keutuhan dari data dan informasi yang dikirimkan, dan juga si pengirim data dan informasi tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut. Untuk memenuhi aspek-aspek dan komponen-komponen dalam pengiriman data, dibutuhkan suatu metode pengamanan data, algoritma kriptografi Asimetrik Rivest Shamir Adleman. Penelitian ini menggunakan metode pengembangan sistem informasi model *System Development Life Cycle* (SDLC), dengan tahapan yang dilakukan meliputi, perencanaan sistem, analisis sistem, desain sistem secara umum, evaluasi dan seleksi sistem, desain sistem secara terinci, implementasi. Penggunaan kriptografi asimetrik dianggap sebagai metode enkripsi yang paling aman saat ini, dimana digunakan dua kunci yang memiliki fungsi untuk melakukan enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki kunci pribadi untuk melakukan pembongkaran terhadap sandi yang dikirimkan untuknya dengan pasangan kunci publiknya. RSA adalah salah satu algoritma asimetrik yang paling populer digunakan dimana dalam penerapannya kunci pribadi dan kunci publik dapat digunakan secara berlawanan dengan tujuan yang berbeda. Pada penelitian tesis ini penulis melakukan pengujian enkripsi dan dekripsi menggunakan 2 (dua) kekuatan kunci RSA 1024 bits dan 2048 bits dengan menguji keefektifan waktu enkripsi dan dekripsi dari 4 (empat) format file yang berbeda.

Kata Kunci: Kriptografi, Algoritma, RSA, Kunci Publik, Kunci Pribadi, Informasi, Data, Enkripsi, Dekripsi.

ABSTRACT

The rapid development of information technology using a computer, resulting in increasingly also problems that accompany the development of these technologies. A data security issue is a factor that must be considered in the development of information technologies further. If we are talking about information technology course also related to the content contained in such information. The information will be delivered must be in accordance with the content that you want to inform. Delivery of data and information should be able to ensure the security of the data and information it sends, so it can be responsible for the transmission of information in terms of confidentiality of data and information, the authenticity of data and information, the integrity of the data and information submitted, as well as the sender of data and information can not be deny that it was he who sent the information. To meet these aspects and components in the delivery of data, we need a method of data security, asymmetric cryptographic algorithm Rivest Shamir Adleman. This study uses a model of information system development System Development Life Cycle (SDLC), with steps being taken include, system planning, system analysis, system design in general, the evaluation and selection system, detailed system design, implementation. The use of asymmetric cryptography is considered as the most secure encryption methods at this time, which used two keys that have a function to perform the encryption and another for decryption. All those who get public key can use it to encrypt a message, while only one person who has the private key to do pembongkaran the password that was sent to him with a public key pair. RSA is one of the most popular asymmetric algorithms used in the application where the private key and public key can be used as opposed to a different destination. On this thesis study authors tested the encryption and decryption using two (2) power and 1024 bits RSA key 2048 bits to test the effectiveness of time encryption and decryption of 4 (four) different file formats.

Keywords: Cryptography, Algorithms, RSA, Public Key, Private Key, Information, Data, Encryption, Decryption.

KATA PENGANTAR

Segala puji penulis ucapkan kepada Allah SWT yang maha mengabulkan permohonan dan maha segalanya. Berkat petunjuk dan rahmat dari-Nya penulis dapat menyelesaikan penelitian tesis ini. Shalawat serta salam penulis persembahkan kepada “Insan Utama” Muhammad SAW sebagai manusia pemimpin umat.

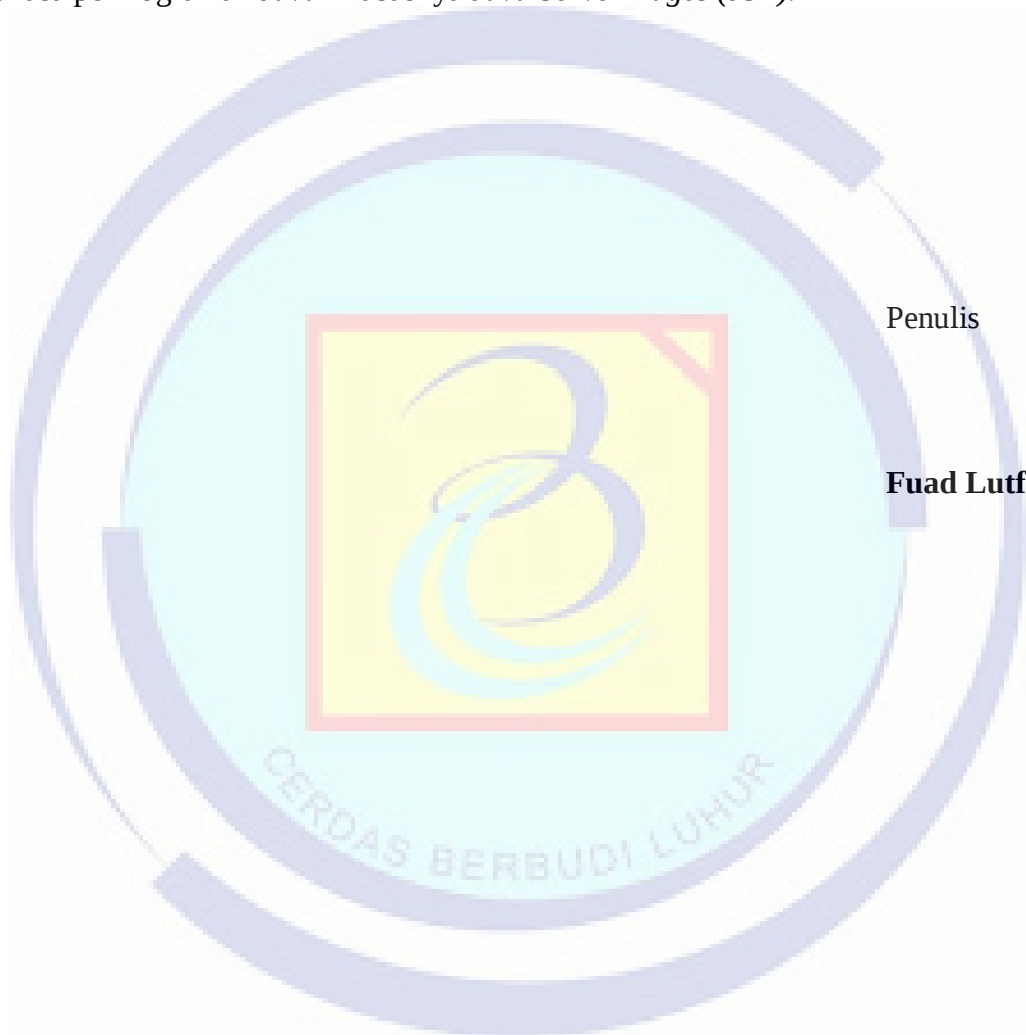
Pengamanan informasi dengan menggunakan metode enkripsi merupakan cara yang biasa digunakan dalam hal pengamanan data dan informasi yang akan di kirimkan, agar data dan informasi yang dikirimkan dapat terjaga kerahasiaannya. Idenya adalah merubah data dan informasi yang dikirimkan menjadi data dan informasi yang tidak dapat dimengerti dimana untuk mengubah kebentuk yang dapat dimengerti menggunakan algoritma yang dapat mengkodekan data yang diinginkan.

Ucapan terima kasih penulis persembahkan kepada semua pihak yang telah membantu penulis dalam menyusun penelitian tesis ini:

1. Dr. Moedjiono, M.Sc, Direktur Program Pascasarjana Universitas Budi Luhur.
2. Dr. Nazori AZ, selaku Ketua Program Studi Magister Ilmu Komputer sekaligus dosen pembimbing tesis penulis yang telah bersedia membimbing dalam penyelesaian penelitian tesisini.
3. Para Dosen pengajar di Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
4. Para staff administrasi di lingkungan Pascasarjana Universitas Budi Luhur.
5. Orang tua, H. Mursyad dan Hj. Mandaini, terima kasih atas dukungan doa, semangat dan kasih sayang yang senantiasa diberikan kepada penulis.
6. Rezka Rahmalia Tanjung, S.KM, istri tercinta yang selalu memberikan semangat, dukungan, dan doa bagi penulis.
7. Ibrahim Halim, anak yang selalu jadi motivasi penulis.

8. Rekan-rekan penulis di Program Magister Ilmu Komputer Universitas Budi Luhur.

Semoga penelitian tesis ini dapat berguna untuk siapa saja yang membacanya, khususnya yang ingin mempelajari masalah keamanan data dan bahasa pemrograman *Java* khususnya *Java Server Pages (JSP)*.



DAFTAR ISI

	halaman
ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
DAFTAR LAMPIRAN	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Masalah Penelitian	2
1.2.1 Identifikasi Masalah	2
1.2.2 Pembatasan Masalah	2
1.2.3 Rumusan Masalah	3
1.3 Tujuan dan Manfaat Penelitian	3
1.3.1 Tujuan Penelitian	3
1.3.2 Manfaat Penelitian	3
1.4 Tata-Urut Penulisan	3
1.5 Daftar Pengertian	4
BAB II LANDASAN TEORI DAN KERANGKA PEMIKIRAN	6
2.1 Tinjauan Pustaka	6
2.1.1 Algoritma	6
2.1.1.1 Pengertian	6
2.1.1.2 Sejarah	7
2.1.1.3 Jenis-Jenis Algoritma	7
2.1.2 Kriptografi	8
2.1.2.1 Pengertian	8
2.1.2.2 Algoritma Sandi	10
2.1.2.2.1 Kunci Simetris	12

2.1.2.2.2	Kunci Asimetris.....	13
2.1.2.3	Fungsi <i>Hash</i> Kriptografis.....	14
2.1.3	Bilangan Prima	14
2.1.4	RSA (Rivest, Shamir, dan Adleman).....	15
2.1.4.1	Pembangkitan Kunci.....	18
2.1.4.2	Proses enkripsi pesan.....	19
2.1.4.3	Proses dekripsi pesan.....	19
2.1.4.4	Beberapa Nilai Yang Tidak Dapat di Enkripsi.....	20
2.1.5	Internet	23
2.1.6	Web.....	25
2.1.6.1	Sejarah <i>Web</i>	25
2.1.6.2	Aplikasi <i>Web</i>	25
2.1.7	HTML	26
2.1.7.1	Dasar-Dasar HTML (HypertextMarkup Language).....	27
2.1.7.2	Struktur Dasar HTML.....	28
2.1.8	<i>Java</i>	29
2.1.8.1	Definisi Singkat	29
2.1.8.2	Deklarasi Package	30
2.1.8.3	Deklarasi <i>Import</i>	30
2.1.8.4	Deklarasi <i>Class</i>	31
2.1.9	<i>JSP</i> (<i>Java Server Pages</i>).....	32
2.1.9.1	Direktif.....	33
2.1.9.2	Scriptlet	34
2.1.9.3	Aksi.....	35
2.2	Tinjauan Studi	36
2.3	Tinjauan Obyek Penelitian.....	42
2.3.1	Algoritma RSA.....	42
2.3.2	Infrastruktur Kunci Publik	43
2.3.3	Sertifikat Digital	44
2.4	Kerangka Konsep dan Pemikiran.....	45
2.5	Hipotesis	48

BAB III METODOLOGI DAN RANCANGAN PENELITIAN.....	49
3.1 Jenis Penelitian.....	49
3.2 Metode Pemilihan Sampel	49
3.3 Metode Pengumpulan Data.....	49
3.4 Instrumentasi.....	50
3.5 Teknik Analisis, Perancangan, Implementasi, dan Pengujian	50
3.5.1 Teknik Analisis.....	50
3.5.2 Perancangan	51
3.5.3 Implementasi	51
3.5.4 Pengujian.....	52
3.5.5 Langkah-Langkah Penelitian.....	52
3.5.6 Jadwal Penelitian	54
BAB IV PEMBAHASAN HASIL PENELITIAN	57
4.1 Analisis	57
4.1.1 Analisa Masalah	57
4.1.2 Temuan-Temuan.....	58
4.1.3 Interpretasi.....	62
4.1.3.1 Enkripsi Kunci Publik.....	62
4.1.3.2 Mekanisme Pembangkitan Kunci.....	63
4.1.3.3 Proses Enkripsi.....	65
4.1.3.4 Proses Dekripsi.....	65
4.1.3.5 Tanda Tangan Digital	66
4.1.3.6 Proses Otentikasi Tanda Tangan Digital	68
4.2 Perancangan Sistem.....	69
4.2.1 Rancangan <i>File</i>	70
4.2.2 Rancangan Input	70
4.2.3 Rancangan <i>Output</i>	71
4.2.4 <i>Flowchart</i> Aplikasi (Alur Aplikasi)	72
4.2.4.1 <i>Flowchart</i> Halaman Utama	72
4.2.4.2 Menu Enkripsi Menggunakan Kunci Pribadi.....	72
4.2.4.3 Menu Dekripsi Menggunakan Kunci Publik	73

4.2.4.4	Menu Enkripsi Menggunakan Kunci Publik.....	74
4.2.4.5	Menu Dekripsi Menggunakan Kunci Pribadi	75
4.2.5	Perancangan Aplikasi Aplikasi RSA	76
4.2.5.1	Rancangan Tampilan Halaman Utama	77
4.2.5.2	Rancangan Tampilan Menu <i>Encrypt</i> Data.....	77
4.2.5.3	Rancangan Tampilan Menu <i>Decrypt</i> Data.....	78
4.2.5.4	Rancangan Tampilan Menu <i>Encrypt</i> Data (Tanda Tangan Digital) 78	
4.2.5.5	Rancangan Tampilan Menu <i>Decrypt</i> Data (Tanda Tangan Digital) 79	
4.2.6	Pengujian Sistem	79
4.2.6.1	Aplikasi Pembangkitan Kunci.....	79
4.2.6.2	Aplikasi Enkripsi Kunci Publik.....	81
4.2.6.3	Proses Dekripsi.....	82
4.2.6.4	Pengujian Enkripsi dan Deskripsi Pada File	83
4.3	Implikasi Penelitian	85
4.3.1	Aspek Sistem.....	86
4.3.2	Aspek Penelitian Lanjut	86
BAB V KESIMPULAN DAN SARAN.....		87
5.1	Kesimpulan	87
5.2	Saran	88
DAFTAR PUSTAKA		89
LAMPIRAN-LAMPIRAN		92

DAFTAR GAMBAR

Gambar	halaman
II.1 Proses Enkripsi dan Dekripsi	9
II.2 Metode Algoritma RSA.....	17
II.3 Fase dari Sebuah Program <i>Java</i>	32
II.4 Kerangka Pemikiran	46
II.5 Kerangka Konsep Proses Enkripsi Data.....	47
II.6 Kerangka Konsep Proses Detesis Data.....	48
III.1 Langkah Langkah Penelitian	52
IV.1 Tampilan Informasi Kunci Publik	63
IV.2 Bentuk dan Isi Informasi Sertifikat Digital	63
IV.3 Activity Diagram Enkripsi Data	64
IV.4 Proses Dekripsi Data	65
IV.5 Metode Pembuatan Tanda Tangan Digital	66
IV.6 Proses Pemeriksaan Message Digest	67
IV.7 Proses Enkripsi Data	68
IV.8 Proses Dekripsi Data	68
IV.9 Rancangan Tampilan Input Kunci Pribadi dan File	70
IV.10 Rancangan Tampilan Input Kunci Publik dan File	70
IV.11 Rancangan Output Hasil Enkripsi dengan Kunci Pribadi	70
IV.12 Rancangan Output Hasil Dekripsi dengan Kunci Publik	71
IV.13 Rancangan Output Hasil enkripsi dengan Kunci Publik	71
IV.14 Rancangan Output Hasil Dekripsi dengan Kunci Pribadi	71
IV.15 Flowchart Halaman Utama	72
IV.16 Flowchart Proses Enkripsi Menggunakan Kunci Publik	73
IV.17 Flowchart Proses Dekripsi Data Menggunakan Kunci Publik	74
IV.18 Flowchart Proses Enkripsi Menggunakan Kunci Publik	75

IV.19 Flowchart Proses Dekripsi Menggunakan Kunci Pribadi	76
IV.20 Model Layout Split Index	77
IV.21 Rancangan Tampilan Halaman Utama	77
IV.22 Rancangan tampilan Menu Enkripsi Data	77
IV.23 Rancangan Tampilan Menu Dekripsi Data	78
IV.24 Rancangan Tampilan Menu Enkripsi Data	78
IV.25 Rancangan Tampilan Menu Dekripsi Data	79
IV.26 Program Pembangkitan Kunci	80
IV.27 File Hasil Program Pembangkitan Kunci	80
IV.28 Pengiriman Kunci Publik Secara Langsung	80
IV.29 Mendapatkan Kunci Publik Melalui Email	81
IV.30 File Yang Telah Terenkripsi	82
IV.31 File Yang Telah Terdekripsi	83

DAFTAR TABEL

Tabel	halaman
II.1 Beberapa Nilai Yang Tidak Dapat di Enkripsi	20
II.2 Perbedaan Bahasa Pemrograman <i>Client Side</i> dengan <i>Server Side</i>	27
II.3 Ringkasan Tinjauan Studi.....	38
II.4 Beberapa Nilai Yang Tidak Dapat di Enkripsi	59
III.1 Jadwal Penelitian.....	54
IV.1 Beberapa Nilai yang Tidak Dapat di enkripsi	58
IV.2 Hasil Pengujian Enkripsi dan Dekripsi Dengan Kekuatan Kunci Publik RSA 1024 bits	83
IV.3 Hasil Pengujian Enkripsi dan Dekripsi Dengan Keukuatan Kunci Publik RSA 2048 bits	84

LAMPIRAN

Lampiran	halaman
1. Source Code Program Pembangkitan Kunci.....	92
2. Source Code Algoritma RSA Enkripsi Kunci Pribadi	93
3. Source Code Algoritma RSA Dekripsi Kunci Publik.....	95
4. Riwayat Hidup Singkat	97



DAFTAR PUSTAKA

- [Amanda 2012] Amanda, Nurul., Simamora., Iskandar, Mohamad Idham. *"Implementasi Algoritma RSA untuk Perlindungan Data pada Server FT"* Naskah Publikasi Politeknik Telkom, 2012.
- [Ariyus 2006] Ariyus, Dony. *Computer Security*. Andi, Yogyakarta: 2006.
- [Burnett 2004] Burnett, Steve and Raine, Stephen. *RSA Security's Official Guide to Cryptography*. Mc Graw Hill Osborn, California: 2004
- [Chalurkar 2011] Chalurkar, Satish N., Khochare, Nilesh , Meshram, B.B. *"Survey on Modular Attack on RSA Algorithm."* IJCEM International Journal of Computational Engineering & Management, Vol. 14, October 2011.
- [Deitel 2003] Deitel, Harvey M. Dan Paul J. Deitel *JavaTM: How To Program*, 5th Edition Prentice Hall, New Jersey: 2003.
- [Flanagan 2000] Flanagan, D. *Java Examples In A Nutshell*. Sabastopol, CA: O'Reilly and Associates, 2000.
- [Firasyan 2011] Firasyan, Terry. *"Penggunaan Algoritma RSA Untuk Keamanan Transaksi Online Berbasis Aplikasi Mobile"* Naskah Publikasi Institut Teknologi 10 Nopember Surabaya, 2012.
- [Hariyanto 2003] Hariyanto, Bambang. *Esensi-Esensi Bahasa Pemrograman Java*. Informatika, Bandung: 2003.
- [Jamgekar 2013] Jamgekar, Rajan.S., Joshi, Geeta Shantanu. *"File Encryption and Decryption Using Secure RSA"* International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319-6378, Volume-1, Issue-4, February 2013.
- [Kadir 2004] Kadir, Abdul. *Dasar Pemrograman Web Dinamis dengan JSP (Java Server Pages)*. Andi, Yogyakarta: 2004.
- [Kadir 2005] _____. *Dasar Pemrograman JavaTM 2*. Andi, Yogyakarta: 2005.
- [Kurniawan 2002] Kurniawan, Budi. *Java for The Web with Servlets, JSP, and EJB: A Developers Guide to J2EE Solutions*, SAMS, 2002.
- [Kurniawan 2004] Kurniawan, Yusuf. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Informatika, Bandung: 2004.