

***HYBRID CRYPTOSYSTEM* UNTUK PENGAMANAN E-DOKUMEN  
MENGUNAKAN ALGORITMA RC4, RSA DAN MD5**

**SKRIPSI**

untuk memenuhi sebagai persyaratan  
mencapai derajat Sarjana S1  
pada jurusan Teknik Informatika



disusun oleh

**Rano Alyas**

**11.11.5425**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2014**

**PERSETUJUAN**

**SKRIPSI**

***HYBRID CRYPTOSYSTEM* UNTUK PENGAMANAN E-DOKUMEN  
MENGUNAKAN ALGORITMA RC4, RSA DAN MD5**

yang dipersiapkan dan disusun oleh

**Rano Alyas**

**11.11.5425**

yang disetujui oleh Dosen Pembimbing Skripsi  
pada Tanggal 21 Februari 2014

**Dosen Pembimbing,**

**Ema Utami, Dr, S.Si, M. Kom**

**NIK. 190302037**

**PENGESAHAN**

**SKRIPSI**

***HYBRID CRYPTOSYSTEM* UNTUK PENGAMANAN E-DOKUMEN  
MENGUNAKAN ALGORITMA RC4, RSA DAN MD5**

yang dipersiapkan dan disusun oleh

**Rano Alyas**

**11.11.5425**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 20 Agustus 2014

**Susunan Dewan Penguji**

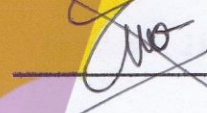
**Nama Penguji**

**Hartatik, S.T, M.Cs**  
**NIK. 190000017**

**Bayu Setiaji, M. Kom**  
**NIK. 190302216**

**Ema Utami Dr., S.Si, M. Kom**  
**NIK. 190302037**

**Tanda Tangan**



Skripsi ini telah diterima sebagai salah satu persyaratan  
Untuk memperoleh gelar Sarjana Komputer  
pada tanggal 25 Agustus 2014



**STMIK AMIKOM YOGYAKARTA**

**Prof. Dr. M. Suyanto, MM.**  
**NIK. 190302001**

## PERNYATAAN

Yang bertandatangan dibawah ini saya :

Nama : Rano Alyas

NIM : 11.11.5425

Jurusan : Teknik Informatika

Selaku mahasiswa STMIK AMIKOM Yogyakarta yang menyusun skripsi ini, saya menyatakan bahwa skripsi ini adalah benar-benar murni hasil karya intelektual saya setelah melakukan pengumpulan data dan mengambil referensi dari berbagai sumber. Dan jika dikemudian hari terjadi pertentangan terhadap skripsi ini, saya siap untuk mempertanggungjawabkannya.

Demikian surat pernyataan keaslian ini saya buat dalam keadaan sadar dan tanpa pengaruh apapun.

Yogyakarta, 21 Februari 2014

Rano Alyas  
NIM 11.11.5425



## HALAMAN MOTO

- ✓ Mulailah sesuatu dengan membaca "Bismillahirrahmanirrahim" dan diakhiri dengan "Alhamdulillahirobbil 'alamin" agar sesuatu yang kita kerjakan di ridhoi Allah SWT.
- ✓ Jadikan kepandaian sebagai kebahagiaan bersama, sehingga mampu meningkatkan rasa ikhlas tuk bersyukur atas kesuksesan.
- ✓ Bersyukurlah atas apa yang kamu miliki saat ini, karena masih banyak orang disekeliling kamu masih kurang beruntung.
- ✓ *"Life is a struggle, there is no life without a struggle."*
- ✓ *"Life is like a wheel, sometimes you will be on the top, sometimes you will be at the bottom. It is not important when we become on the top or at the bottom. But the most important is syukur when success and shabar when fail."*
- ✓ *just do it, it will go away (Skripsi - Pendadaran - Yudisium - Wisuda), and in the end we will always say "Cuma kayak gini toh"*

## HALAMAN PERSEMBAHAN

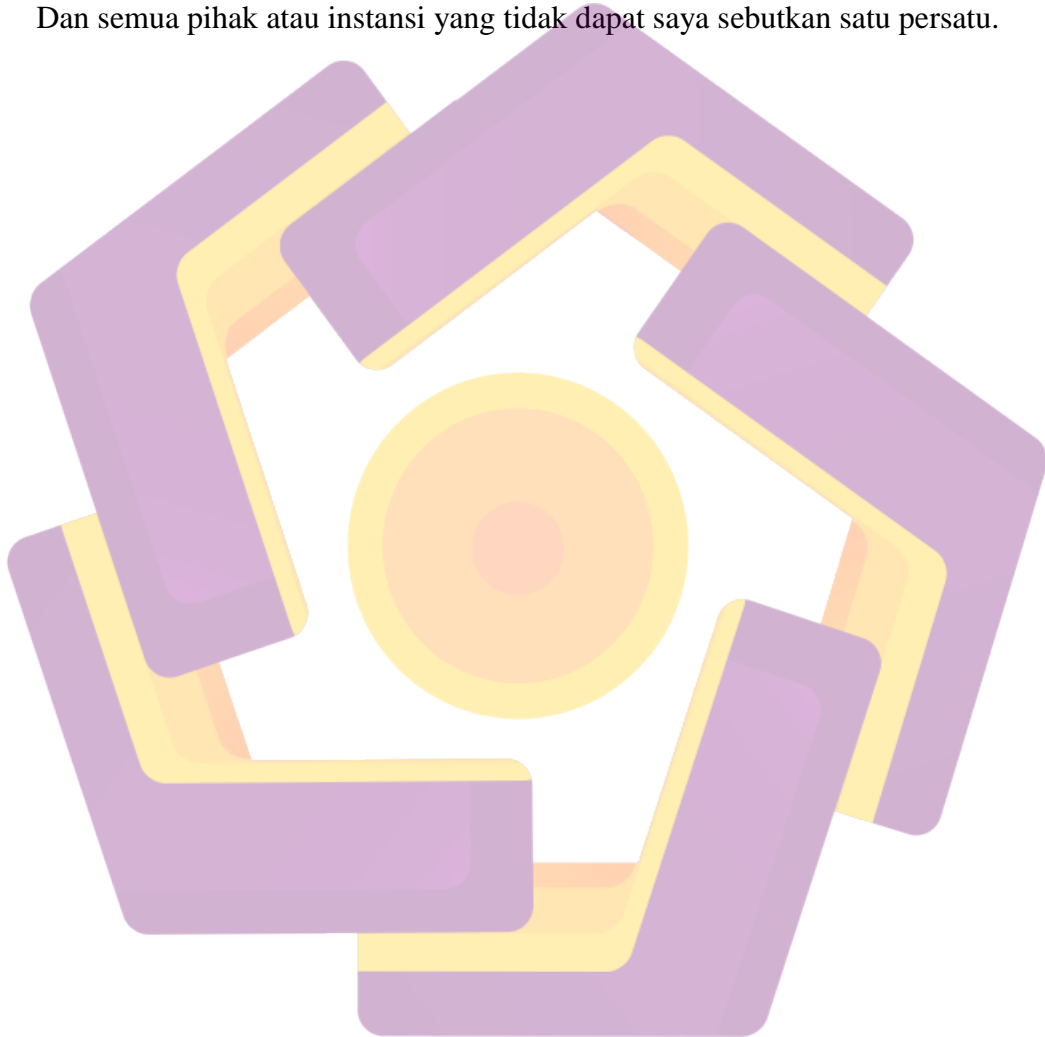
Puji syukur senantiasa terucap kehadirat Alloh SWT, yang telah melimpahkan nikmat yang luar biasa kepada setiap hamba-Nya. Shalawat serta salam selalu tercurah kepada Nabi Muhammad SAW.

Skripsi ini saya persembahkan kepada pihak-pihak yang telah memberikan dukungan. Skripsi ini di dedikasikan untuk :

1. Kedua Orang Tua, yang telah memberikan dukungan baik moril maupun materiil. Untuk doa dan perhatian serta kesabarannya membimbing dan mengajarkan segala hal.
2. Mas dan Mba ku tercinta, pakhde, budhe, semua keluarga besar baik dari bapak maupun ibu. Terima kasih atas petuah, nasihat, serta doanya.
3. Keponakan ku tersayang, dhe Vera, Danniz, Arqi, dan dhe Njey, terima kasih atas senyuman, candaan, dan tingkah lucu kalian.
4. Teman-teman 11-SITI-11, yang telah banyak memberikan kenangan di kampus ungu tercinta. Terima kasih atas dukungan, kritik, dan sarannya semoga kita semuanya sukses dunia akhirat.Amin. .
5. Seluruh Keluarga Besar Badan Eksekutif Mahasiswa AMIKOM Kabinet “Normalisasi kontribusi” dan “Sinergis Berkarakter”. Terima kasih atas suasana kekeluargaannya selama ini, dukungan dan doanya.
6. Teman-teman ku, Aris, Prast, Ardun, Iyan, Nana, Ninda, Mas Erwandy, Akhid, Chandra, Devi, Yunis dan Fikri, Wina yang di Bumiayu. Terima kasih tingkah gila dan lucu kalian.semoga kita jadi sahabat sejati.

7. Teman-teman Asisten (HS II, Stuktur Data, Pemrog Lanjut, PBO 2), Kontrakan “Rumah Kece”, Fighter School, Public Relations School, Forum Asisten, yang telah *mensupport* dan memberikan share ilmu serta doanya.

Dan semua pihak atau instansi yang tidak dapat saya sebutkan satu persatu.



## KATA PENGANTAR

Puji syukur kehadiran Tuhan Yang Maha Esa yang telah memberikan rahmat dan hidayahnya, sehingga penulisan Skripsi ini dapat penulis selesaikan.

Pembuatan Skripsi ini guna memenuhi persyaratan akademis untuk memperoleh gelar Sarjana Komputer di STMIK AMIKOM Yogyakarta.

Penulis sangat menyadari bahwa dalam penulisan Skripsi ini sangat jauh dari kesempurnaan, karena keterbatasan kemampuan dan pengetahuan yang penulis miliki, dan juga walaupun Skripsi ini sangat sederhana namun tanpa bantuan dari berbagai pihak tentunya penulis akan mengalami kesulitan. Oleh karena itu dalam kesempatan ini, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. M.Suyanto, Prof., Dr., MM. selaku Ketua STMIK AMIKOM Yogyakarta.
2. Ema Utami, Dr., S.Si., M.Kom. selaku Dosen Pembimbing yang telah meluangkan waktunya untuk membimbing penulis dengan penuh kesabaran.
3. Ibu Hartatik, M.Cs, Bpk.Hastari Utama, S.Kom., M.Cs dan Bapak Emha Taufiq Luthfi, M.Kom. yang juga telah membantu penulis dalam menyelesaikan Skripsi ini.
4. Segenap staf pengajar STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmunya dan pengalaman selama penulis kuliah.
5. Orang Tua penulis yang telah mendoakan dan memberi dukungannya.

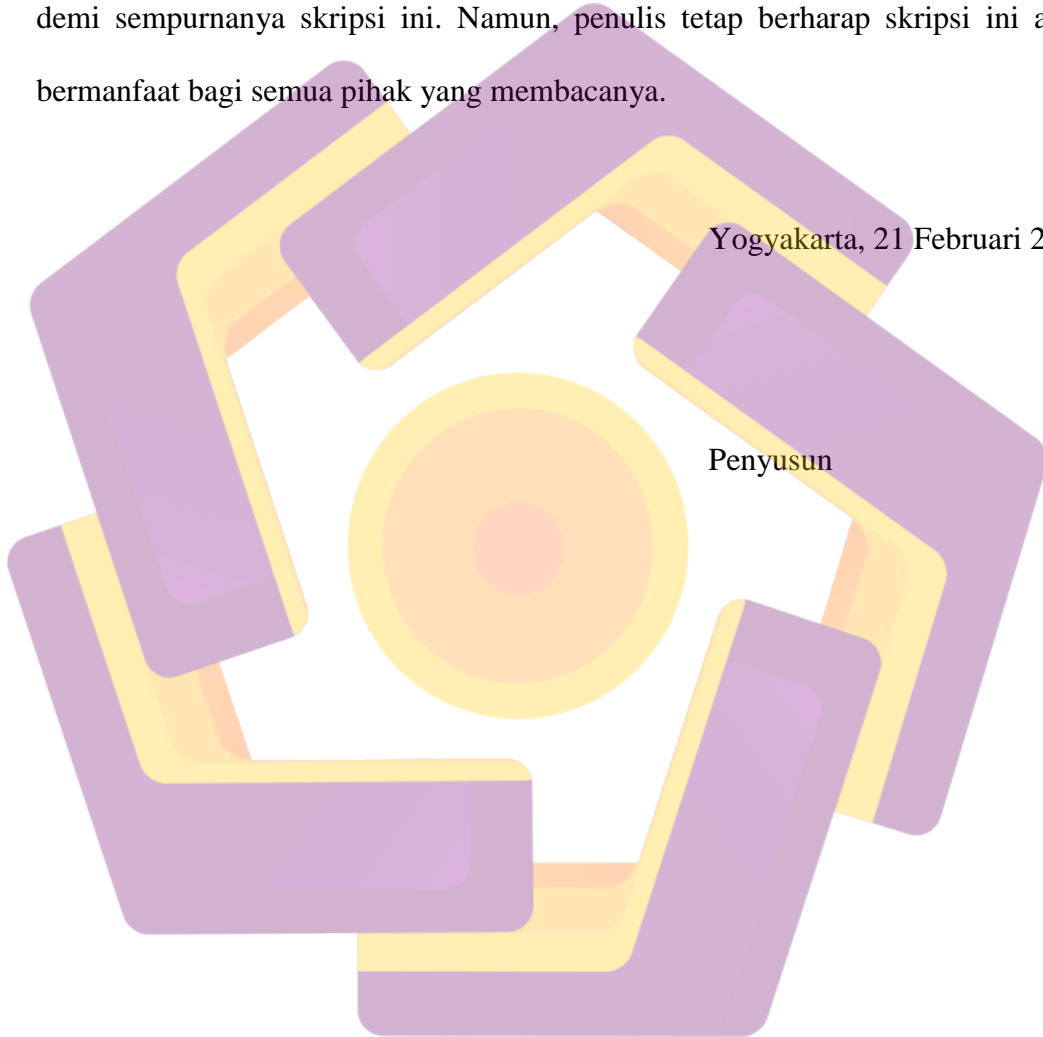


6. Seluruh pihak yang telah membantu penulis dalam menyelesaikan Skripsi ini.

Penulis menyadari bahwa pembuatan Skripsi ini jauh dari sempurna, oleh karena itu saran dan kritik yang bersifat membangun sangat penulis harapkan demi sempurnanya skripsi ini. Namun, penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 21 Februari 2014

Penyusun



## DAFTAR ISI

<b>PERSETUJUAN</b> .....	Error! Bookmark not defined.
<b>PENGESAHAN</b> .....	Error! Bookmark not defined.
<b>PERNYATAAN</b> .....	<b>iii</b>
<b>HALAMAN MOTO</b> .....	<b>v</b>
<b>HALAMAN PERSEMBAHAN</b> .....	<b>vi</b>
<b>KATA PENGANTAR</b> .....	<b>viii</b>
<b>DAFTAR ISI</b> .....	<b>x</b>
<b>DAFTAR TABEL</b> .....	<b>xiv</b>
<b>DAFTAR GAMBAR</b> .....	<b>xv</b>
<b>INTISARI</b> .....	<b>xviii</b>
<b>ABSTRACT</b> .....	<b>xix</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	5
1.6 Metodologi Penelitian .....	6
1.7 Sistematika Penulisan.....	7
<b>BAB II LANDASAN TEORI</b> .....	<b>9</b>
2.1 Dokumen .....	9
2.1.1 Pengertian Dokumen .....	9
2.1.2 Jenis-jenis Dokumen.....	10
2.1.2.1 Jenis dokumen dari segi pemakaian.....	10
2.1.2.2 Jenis dokumen dari segi fungsinya .....	11
2.1.2.3 Jenis dokumen dari segi ruang lingkupnya .....	11
2.1.3 E-Dokumen (Elektronik Dokumen) .....	12

2.2	Konsep Dasar Kriptografi .....	12
2.2.1	Pengertian Kriptografi .....	13
2.2.2	Tujuan Kriptografi .....	15
2.2.3	Cryptosystem dan Hybrid Cryptosystem .....	15
2.2.3.1	Symetric Cryptosystem .....	16
2.2.3.2	Assymmetric Criptosystem .....	17
2.3	RC4.....	17
2.4	RSA .....	20
2.5	MD5 .....	22
2.6	Definisi Program dan Bahasa Pemrograman .....	24
2.7	Java.....	24
2.7.1	Karakteristik <i>Java</i> .....	26
2.7.2	Teknologi Java .....	27
2.7.3	Java Class Library .....	28
2.7.4	IDE NetBean .....	30
2.8	Teori Analisis SWOT.....	31
2.9	UML.....	32
2.9.1	Usecase Diagram.....	32
2.9.2	Class Diagram .....	33
2.9.3	Sequence Diagram .....	35
2.9.4	Activity Diagram .....	35
<b>BAB III</b>	<b>ANALISIS DAN PERANCANGAN.....</b>	<b>37</b>
3.1	Gambaran Umum Aplikasi.....	37
3.1.1	Model Sistem Aplikasi Lama .....	38
3.1.2	Model Sistem Aplikasi Baru.....	38
3.2	Analisis SWOT .....	38
3.2.1	Kekuatan ( <i>Strengths</i> ) .....	39
3.2.2	Kelemahan ( <i>Weakness</i> ).....	40
3.2.3	Peluang ( <i>Opportunities</i> ).....	40
3.2.4	Ancaman ( <i>Threats</i> ) .....	41
3.3	Analisis Kebutuhan Sistem .....	42

3.3.1	Analisis Kebutuhan Fungsional.....	42
3.3.2	Analisis Kebutuhan Non Fungsional.....	43
3.3.2.1	Analisis kebutuhan perangkat keras ( <i>hardware</i> ) .....	43
3.3.2.2	Analisis kebutuhan perangkat lunak ( <i>software</i> ).....	44
3.3.2.3	Analisis kebutuhan SDM ( <i>brainware</i> ).....	45
3.4	Analisis Kelayakan Sistem.....	45
3.5	Analisis Data .....	46
3.5.1	Hasil Hitung Manual RC4 .....	46
3.5.2	Hasil Hitung Manual RSA.....	52
3.5.3	Hasil Hitung Manual MD5 .....	54
3.6	Perancangan Sistem.....	55
3.6.1	Perancangan Prosedural.....	55
3.6.2	Perancangan Proses .....	58
3.6.2.1	Use Case Diagram.....	58
3.6.2.2	Activity Diagram .....	60
3.6.2.3	Sequence Diagram .....	67
3.6.2.4	Class Diagram .....	71
3.6.3	Perancangan <i>Interface</i> / Antarmuka .....	72
3.6.3.1	Tampilan Splashscreen atau Loading .....	72
3.6.3.2	Tampilan Menu Utama .....	73
3.6.3.3	Tampilan Menu Enkripsi .....	74
3.6.3.4	Tampilan Menu Dekripsi .....	75
3.6.3.5	Tampilan Menu Bantuan / <i>Help</i> .....	76
3.6.3.6	Tampilan Menu Tentang / <i>About</i> .....	77
3.6.3.7	Tampilan Menu Keluar / <i>Exit</i> .....	78
<b>BAB IV IMPLEMENTASI DAN PEMBAHASAN .....</b>		<b>79</b>
4.1	Implementasi .....	79
4.1.1	Implementasi Algoritma .....	79
4.1.1.1	Algoritma RC4.....	80
4.1.1.2	Algoritma RSA .....	82
4.1.1.3	Algoritma MD5.....	84

4.1.2	Implementasi Interface .....	86
4.1.2.1	Tampilan SplashScreen .....	86
4.1.2.2	Tampilan Menu Utama .....	87
4.1.2.3	Tampilan Enkripsi .....	88
4.1.2.4	Tampilan Dekripsi .....	89
4.1.2.5	Tampilan Bantuan / <i>Help</i> .....	90
4.1.2.6	Tampilan Tentang Aplikasi / <i>About</i> .....	91
4.1.2.7	Tampilan Keluar .....	92
4.2	Pembahasan .....	93
4.2.1	Pembahasan Program .....	93
4.2.1.1	Kode Program Pada Splash Screen .....	93
4.2.1.2	Kode Program Untuk Mencari File .....	96
4.2.1.3	Kode Program Untuk Membuat Tandatangan MD5 pada Button ..	96
4.2.1.4	Kode Program Untuk Menyimpan Dalam Ekstensi .zip .....	97
4.2.2	Pengujian Aplikasi .....	99
4.2.3	Pengujian Program .....	114
4.2.3.1	Whitebox Testing .....	114
4.2.3.2	Blackbox Testing .....	115
4.2.4	Hasil Pengujian Aplikasi .....	117
<b>BAB V</b>	<b>PENUTUP .....</b>	<b>121</b>
5.1	Kesimpulan .....	121
5.2	Saran .....	122
<b>DAFTAR PUSTAKA .....</b>		<b>124</b>



## DAFTAR TABEL

Tabel 2.1 <i>Package-Package J2SE</i> .....	28
Tabel 2.2 Simbol-Simbol <i>Usecase Diagram</i> .....	32
Tabel 2.3 Simbol-Simbol <i>Class Diagram</i> .....	34
Tabel.2.4 Simbol-Simbol <i>Sequence Diagram</i> .....	35
Tabel 2.5 Simbol-Simbol <i>Activity Diagram</i> .....	36
Tabel 3.1 Kesimpulan Analisis SWOT.....	41
Tabel 3.2 Spesifikasi Komputer.....	44
Tabel 3.3 Spesifikasi Perangkat Lunak( <i>Software</i> ).....	44
Tabel 3.4 Kode ASCII Plainteks.....	52
Tabel 3.5 Proses XOR Kunci Enkripsi Dengan Plainteks .....	52
Tabel 3.6 Proses XOR Kunci Dekripsi Dengan Cipherteks .....	52
Tabel 4.1 BlackBox Testing .....	116
Tabel 4.2 Hasil Ujicoba Aplikasi Pada Spek Komputer Yang Berbeda.....	118
Tabel 4.3 Hasil Kecepatan Enkripsi Dengan Ukuran File Yang Berbeda.....	119

## DAFTAR GAMBAR

Gambar 2.1 Proses Kriptografi .....	14
Gambar 2.2 <i>Symmetric Cryptosystem</i> .....	16
Gambar 2.3 <i>Assymmetric Cryptosystem</i> .....	17
Gambar 2.4 Pembuatan Algoritma MD5 .....	24
Gambar 3.1 <i>Flowchart</i> Enkripsi .....	56
Gambar 3.2 <i>Flowchart</i> Dekripsi .....	57
Gambar 3.3 <i>Usecase Diagram</i> .....	58
Gambar 3.4 <i>Activity Diagram</i> <i>SplashScreen</i> .....	61
Gambar 3.5 <i>Activity Diagram</i> Enkripsi .....	62
Gambar 3.6 <i>Activity Diagram</i> Dekripsi .....	63
Gambar 3.7 <i>Activity Diagram</i> Bantuan .....	64
Gambar 3.8 <i>Activity Diagram</i> Tentang .....	65
Gambar 3.9 <i>Activity Diagram</i> Keluar .....	66
Gambar 3.10 <i>Sequence Diagram</i> <i>SplashScreen</i> .....	67
Gambar 3.11 <i>Sequence Diagram</i> Menu Enkripsi .....	68
Gambar 3.12 <i>Sequence Diagram</i> Menu Dekripsi .....	69
Gambar 3.13 <i>Sequence Diagram</i> Menu Bantuan .....	70
Gambar 3.14 <i>Sequence Diagram</i> Menu Tentang .....	71
Gambar 3.15 <i>Class Diagram</i> .....	72
Gambar 3.16 Rancang <i>SplashScreen/Loading</i> .....	73
Gambar 3.17 Rancang Menu Utama .....	73
Gambar 3.18 Rancang Menu Enkripsi .....	74
Gambar 3.19 Rancang Menu Dekripsi .....	75
Gambar 3.20 Rancang Menu Bantuan / <i>Help</i> .....	76

Gambar 3.21 Rancang Menu Tentang / <i>About</i> .....	77
Gambar 3.22 Rancang Menu Keluar / <i>Exit</i> .....	78
Gambar 4.1 Tampilan <i>SplashScreen</i> .....	87
Gambar 4.2 Tampilan Menu Utama .....	88
Gambar 4.3 Tampilan Menu Enkripsi.....	89
Gambar 4.4 Tampilan Menu Dekripsi .....	90
Gambar 4.5 Tampilan Menu Bantuan / <i>Help</i> .....	91
Gambar 4.6 Tampilan Menu Tentang Aplikasi / <i>About</i> .....	92
Gambar 4.7 Tampilan Keluar / <i>Exit</i> .....	92
Gambar 4.8 Tampilan Pilih Aplikasi Dalam Media Penyimpanan.....	100
Gambar 4.9 Tampilan <i>SplashScreen</i> Pada Saat Aplikasi Dijalankan .....	100
Gambar 4.10 Tampilan Pilih Menu Enkripsi .....	101
Gambar 4.11 Tampilan <i>Browse File</i> .....	102
Gambar 4.12 Tampilan Kesalahan Jika Belum Memasukan Kunci RC4.....	103
Gambar 4.13 Tampilan Kunci Lebih Dari 20 Karakter .....	104
Gambar 4.14 Tampilan Enkripsi Berhasil.....	105
Gambar 4.15 Tampilan Proses Enkripsi RC4, RSA dan MD5 .....	106
Gambar 4.16 Tampilan File Simpan.....	107
Gambar 4.17 Tampilan File Berhasil Disimpan .....	108
Gambar 4.18 Tampilan File .zip .....	108
Gambar 4.19 Tampilan Pilih Menu Dekripsi.....	109
Gambar 4.20 Tampilan Input Private Key dan Cipherteks RSA.....	109
Gambar 4.21 Tampilan Hasil Dekripsi RSA .....	110
Gambar 4.22 Tampilan Pilih File Dekripsi.....	110
Gambar 4.23 Tampilan Dekripsi Berhasil .....	111

Gambar 4.24 Tampilan Buat Tandatangan MD5.....	111
Gambar 4.25 Tampilan Perbandingan Tandatangan MD5 .....	112
Gambar 4.26 Tampilan Setelah di RESET .....	112
Gambar 4.27 File Sebelum Dan Sesudah Dienkripsi.....	113
Gambar 4.28 <i>WhiteBox Testing</i> .....	115
Gambar 4.29 Grafik Kecepatan Enkripsi Dan Dekripsi Pada Komputer Yang Berbeda .....	118
Gambar 4.30 Grafik Kecepatan Enkripsi Pada Ukuran File Yang Berbeda.....	119



## INTISARI

Pertukaran dokumen di dunia maya sudah banyak digunakan dalam transaksi komersial. Oleh karena itu, dokumen merupakan peranan penting yang harus di amankan oleh setiap *user*. Keamanan dari suatu dokumen merupakan hal yang perlu diperhatikan dalam menjaga kerahasiaan informasi, terutama untuk informasi yang isinya hanya boleh diketahui oleh pihak yang berwenang saja. Pengiriman data atau informasi tanpa dilakukan pengamanan akan beresiko terhadap penyadapan dan informasi yang ada di dalamnya dapat mudah diketahui oleh pihak-pihak yang tidak berwenang.

Salah satu cara untuk mengamankan dokumen adalah dengan menggunakan algoritma kriptografi. Prinsip pengamanan dokumen ini adalah bagaimana sistem dapat mengamankan proses penyimpanan dan pengiriman dokumen menggunakan *hybrid cryptosystem*. Pada penelitian ini, penggunaan *hybrid cryptosystem* merupakan gabungan algoritma RC4, RSA dan MD5. Adapun tahapan pengamanan dokumen ini meliputi tiga tahapan yaitu proses pengamanan data, pengamanan kunci, dan pengujian integritas sebuah berkas.

Aplikasi yang dibangun dapat melakukan enkripsi dan dekripsi file / dokumen. Hasil pengujian yang telah dilakukan dapat disimpulkan bahwa aplikasi telah mampu menunjukkan dan melakukan enkripsi dan dekripsi pada dokumen file. Kinerja aplikasi ini dapat disimpulkan bahwa semakin besar ukuran file yang dienkripsi maka semakin lama prosesnya dan semakin tinggi spek komputer yang digunakan maka semakin cepat pula proses enkripsi dan dekripsi yang diproses dalam aplikasi SecureDoc.

**Kata Kunci :** *Hybrid Cryptosystem*, Kriptografi, RC4, RSA, MD5 dan Dokumen.



## ABSTRACT

*The exchange of documents in cyberspace already widely used in commercial transactions . Therefore , the document is an important role that must be secured by each user . Security of a document is to be considered in maintaining the confidentiality of information , especially for the contents of information that should only be known by the authorities alone . Delivery of data or information without any security will be at risk to eavesdropping and the information in it can be easily identified by parties who are not authorized .*

*One way to secure the document is to use a cryptographic algorithm . The principle of security of this document is how the system can secure the storage and delivery of documents using a hybrid cryptosystem . In this research , the use of hybrid cryptosystem is combination the RC4 algorithm , RSA and MD5. The stages of the security document includes three stages: data security processes , security locks , and testing the integrity of a file .*

*Applications built can perform encryption and decryption of file / document. The results of the testing that has been done can be concluded that the application has been able to show and perform encryption and decryption on a document of file. The performance of these applications can be concluded that the larger the file size the longer the process in encrypted and the higher spec computer used the faster encryption and decryption processes are processed on SecureDoc applications.*

**Keywords** : Hybrid Cryptosystem , Cryptography , RC4 , RSA , MD5 and Documents.