

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA DAN AES
UNTUK ENKRIPSI PESAN DAN FILE PADA
APLIKASI EMAIL BERBASIS DESKTOP**

SKRIPSI



disusun oleh

Bima Sakti

14.11.8008

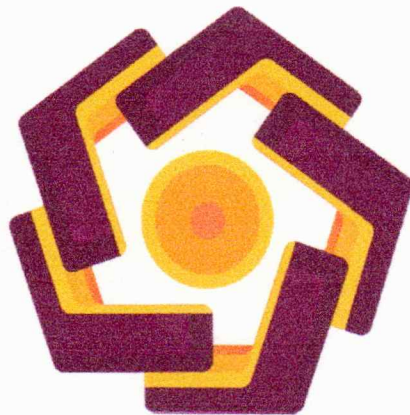
**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
2018**



**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA DAN AES
UNTUK ENKRIPSI PESAN DAN FILE PADA
APLIKASI EMAIL BERBASIS DESKTOP**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Bima Sakti

14.11.8008

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**



PERSETUJUAN

SKRIPSI

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA DAN AES
UNTUK ENKRIPSI PESAN DAN FILE PADA APLIKASI EMAIL
BERBASIS DESKTOP**

yang dipersiapkan dan disusun oleh

Bima Sakti

14.11.8008

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 September 2018

Dosen Pembimbing,



Bayu Setiaji, M.Kom.
NIK. 190302216

PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA DAN AES UNTUK ENKRIPSI PESAN DAN FILE PADA APLIKASI EMAIL BERBASIS DESKTOP

yang dipersiapkan dan disusun oleh

Bima Sakti

14.11.8008

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 September 2018

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Bayu Setiaji, M.Kom.
NIK. 190302216

Agus Fatkhurohman, M.Kom.
NIK. 190302249

Windha Mega Pradnya D, M.Kom.
NIK. 190302185



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 September 2018

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si., M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 24 September 2018



Bima Sakti

NIM. 14.11.8008

MOTTO

وَالْعَصْرُ ۚ إِنَّ الْإِنْسَانَ لَفِي خُسْرٍ ۚ إِلَّا الَّذِينَ آمَنُوا وَعَمِلُوا
الصَّالِحَاتِ وَتَوَاصَوْا بِالْحَقِّ ۚ وَتَوَاصَوْا بِالصَّبْرِ

"Demi masa, sungguh, manusia berada dalam kerugian, kecuali orang-orang yang beriman dan mengerjakan kebajikan serta saling menasihati untuk kebenaran dan saling menasihati untuk kesabaran."

(QS. Al-'Asr : 1-3)



PERSEMBAHAN

Alhamdulillah Rabbil'alamiin, Sembah sujud serta syukur kepada Allah SWT. Atas karunia serta kemudahan yang Engkau berikan akhirnya skripsi yang sederhana ini dapat terselesaikan. Sholawat dan salam selalu terlimpahkan kepada Rasulullah Muhammad SAW yang kita nantikan syafaatnya di hari akhir kelak.

Skripsi ini penulis persembahkan kepada :

1. Orang tua saya, Ibu Maryati dan Bapak Maryanto yang selalu memberikan kasih sayang, membimbing, serta memberikan do'a dan semangat kepada penulis dan tak pernah lelah mendidik penulis untuk selalu mencari ilmu, belajar, ibadah, dan berdo'a.
2. Keluarga saya, yang selalu memberikan dukungan, motivasi, serta do'a kepada penulis.
3. Teman spesial saya yang tidak bisa penulis sebutkan, yang selalu sabar, perhatian, memberikan motivasi, arahan, dukungan serta do'a yang diberikan kepada penulis untuk segera menyelesaikan skripsi ini.
4. Teman-teman Universitas Amikom Yogyakarta, yang selalu memberikan arahan, semangat, bimbingan dan dukungan kepada penulis dalam penyelesaian skripsi ini.
5. Almameter saya, Universitas Amikom Yogyakarta.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ. أَشْهَدُ أَنْ لَا إِلَهَ إِلَّا اللَّهُ وَ أَشْهَدُ أَنَّ مُحَمَّدًا رَسُولُ اللَّهِ. اللَّهُمَّ صَلِّ وَسَلِّمْ عَلَى مُحَمَّدٍ وَعَلَى آلِهِ وَصَحْبِهِ أَجْمَعِينَ. أَمَّا بَعْدُ.

Alhamdulillah Rabbil'alamiin, Puji syukur penulis panjatkan kehadiran Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **“Implementasi Algoritma Kriptografi Rsa Dan Aes Untuk Enkripsi Pesan Dan File Pada Aplikasi Email Berbasis Desktop”**. Sholawat serta salam semoga senantiasa tercurah kepada junjungan kita Nabi Muhammad ﷺ suri tauladan seluruh umat hingga akhir zaman. Skripsi ini disusun untuk memenuhi salah satu persyaratan memperoleh gelar Sarjana Komputer Universitas Amikom Yogyakarta. Dalam penyusunan skripsi ini, penulis banyak mendapatkan bantuan dari berbagai pihak, baik moril maupun materiil. Pada kesempatan yang baik ini perkenankanlah penulis mengucapkan terimakasih yang setulus-tulusnya kepada:

1. Rektor Universitas Amikom Yogyakarta yang telah memberi kesempatan kepada penulis untuk menempuh pendidikan di Universitas Amikom Yogyakarta.
2. Ibu Krisnawati, S.Si, MT., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta beserta para staf-stafnya yang telah membantu penulis menyelesaikan tugas akhir skripsi ini.

3. Bapak Sudarmawan, MT., selaku Ketua Program Studi Informatika sekaligus telah memberikan nasihat dan bimbingan selama menempuh Program Strata Satu Informatika.
4. Bapak Erik Hadi Saputra, S.Kom, M.Eng., selaku Dosen Penasehat Akademik sekaligus yang telah memberikan petunjuk, arahan, bimbingan, saran, dan waktu dalam proses pembuatan skripsi ini.
5. Bapak Bayu Setiaji, M.Kom., selaku Dosen Pembimbing Skripsi dan yang telah memberikan bimbingan, arahan, motivasi, inspirasi, nasihat, serta waktu dan tenaga selama proses penyelesaian skripsi ini.
6. Seluruh Dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu, inspirasi, dan motivasi pada saat kegiatan kuliah maupun saat di luar kuliah.
7. Ayahanda Maryanto dan Ibunda tercinta Maryati serta segenap keluarga besar, terima kasih atas semua yang telah kalian berikan, terima kasih atas segala bimbingan, kepercayaan, motivasi, harapan, serta doa yang tak kunjung henti.
8. Teman-teman Teknik Informatika 2014, sahabat perjuanganku semuanya yang tak bisa aku sebut satu persatu. Terima kasih telah mengisi perjalanan hidupku.
9. Teman spesial yang telah menemani perjalanan pembuatan skripsi, terima kasih atas nasihat, motivasi, arahan, serta doa yang tak kunjung henti.

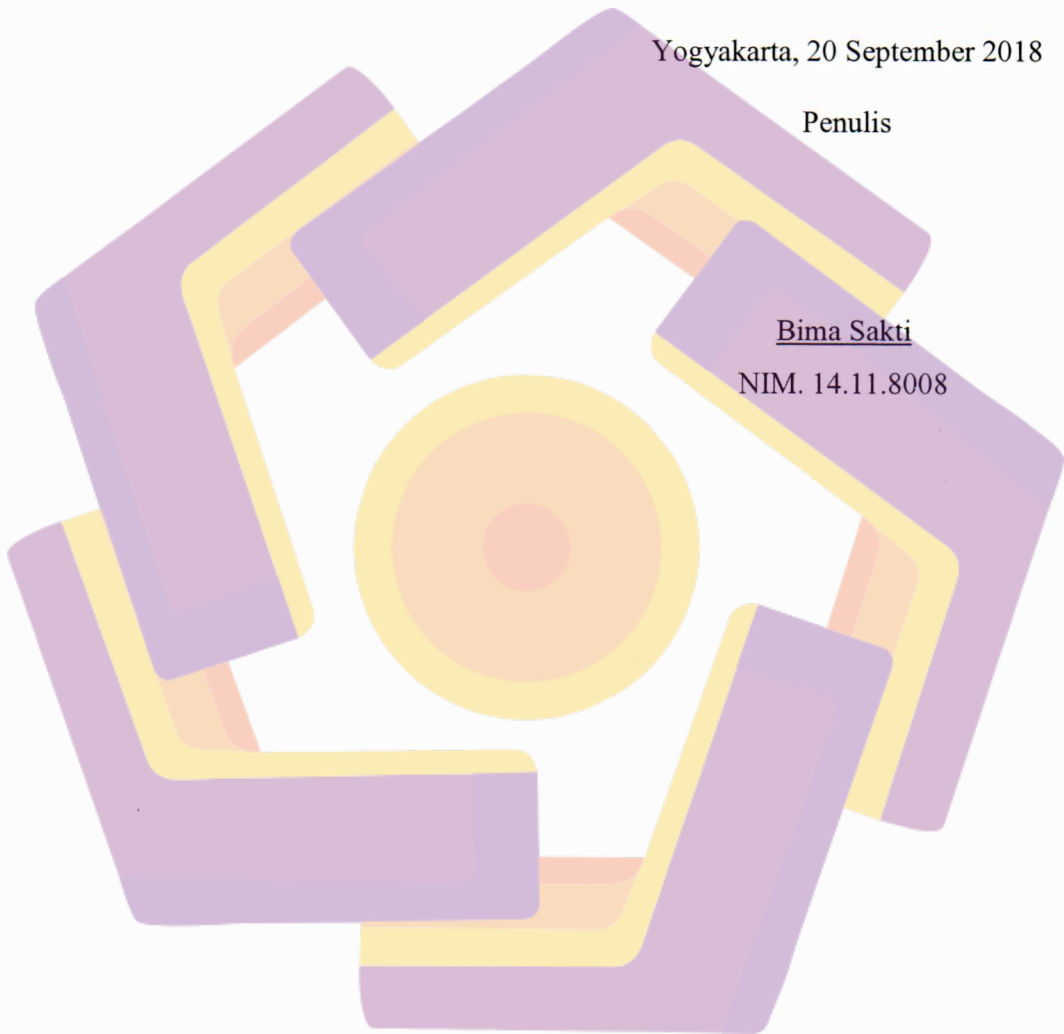
Proses belajar ini tentu tak luput dari kekurangan maupun kesalahan, begitu juga dalam proses penyusunan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi penulis maupun bagi yang membaca.

Yogyakarta, 20 September 2018

Penulis

Bima Sakti

NIM. 14.11.8008



DAFTAR ISI

PERSETUJUAN	II
PENGESAHAN	III
PERNYATAAN	IV
MOTTO	V
PERSEMBAHAN	VI
KATA PENGANTAR	VII
DAFTAR ISI	X
DAFTAR TABEL	XV
DAFTAR GAMBAR	XVII
INTISARI	XX
<i>ABSTRACT</i>	XXI
BAB I PENDAHULUAN	1
1.1 LATAR BELAKANG MASALAH	1
1.2 RUMUSAN MASALAH	2
1.3 BATASAN MASALAH	3
1.4 MAKSUD DAN TUJUAN PENULISAN	5
1.5 MANFAAT PENULISAN	5
1.6 METODE PENULISAN	6
1.7 SISTEMATIKA PENULISAN	8
BAB II LANDASAN TEORI	9
2.1 KAJIAN PUSTAKA	9
2.2 DASAR TEORI	13
2.2.1 Email	13
2.2.1.1 Pengertian Email	13
2.2.1.2 SMTP	13
2.2.1.3 IMAP	13
2.2.2 Kriptografi	14
2.2.2.1 Pengertian Kriptografi	14
2.2.2.2 Sejarah Kriptografi	14

2.2.2.3	Algoritma Kriptografi.....	15
2.2.2.3.1	Kunci Simetris.....	17
2.2.2.3.2	Kunci Asimetris.....	17
2.2.2.3.3	Hash <i>Function</i>	18
2.2.2.4	RSA.....	19
2.2.2.4.1	Pengertian RSA.....	19
2.2.2.4.2	Pembangkit Kunci RSA.....	19
2.2.2.5	AES.....	20
2.2.3	XML (eXtensible Markup Language).....	21
2.2.3.1	Pengertian XML.....	21
2.2.3.2	Struktur Dokumen XML.....	21
2.2.4	UML (Unified Modeling Language).....	22
2.2.4.1	Pengertian UML.....	22
2.2.4.2	Diagram UML.....	23
2.2.4.3	Use Case Diagram.....	24
2.2.4.4	Activity Diagram.....	26
2.2.4.5	Class Diagram.....	28
2.2.4.6	Sequence Diagram.....	31
2.2.5	SDLC.....	34
2.2.5.1	Sejarah SDLC.....	34
2.2.5.2	Pengertian SDLC.....	34
2.2.5.3	Model Waterfall.....	37
2.2.5.3.1	<i>Analysis</i> (Analisis Kebutuhan Perangkat Lunak).....	37
2.2.5.3.2	<i>Design</i> (Perancangan Sistem).....	38
2.2.5.3.3	<i>Code</i> (Pembuatan kode program).....	38
2.2.5.3.4	<i>Test</i> (Pengujian).....	38
2.2.5.3.5	<i>Support</i> (Pendukung) atau <i>maintenance</i> (pemeliharaan).....	38
BAB III ANALISIS DAN PERANCANGAN.....		38
3.1	TINJAUAN UMUM APLIKASI CRYPT-MAIL.....	38
3.2	ANALISIS SISTEM.....	38
3.2.1	Analisis Kebutuhan Sistem.....	38

3.2.1.1	Analisis Kebutuhan Fungsioal	38
3.2.1.2	Analisis Kebutuhan non-Fungsioal	40
3.2.1.2.1	Kebutuhan Operasional (<i>Operational Requirement</i>).....	40
3.2.1.2.2	Kebutuhan performa (<i>performance requirement</i>)	40
3.2.1.2.3	Kebutuhan keamanan (<i>security requirement</i>)	41
3.2.1.2.4	Kebutuhan Politik dan Budaya (<i>Cultural and Political Requirement</i>).....	41
3.2.2	Analisis Kelayakan Sistem	41
3.2.2.1	Analisis Kelayakan Teknis.....	41
3.2.2.2	Analisis Kelayakan Operasional.....	41
3.2.2.3	Analisis Kelayakan Hukum.....	42
3.3	PERANCANGAN SISTEM	42
3.3.1	UML (Unified Modeling Language).....	42
3.3.1.1	<i>Use Case Diagram</i>	42
3.3.1.2	<i>Activity Diagram</i>	45
3.3.1.2.1	<i>Activity Diagram</i> Konfigurasi Akun Email.....	45
3.3.1.2.2	<i>Activity Diagram</i> Kirim Email.....	46
3.3.1.2.3	<i>Activity Diagram</i> Tampil Email Terkirim.....	48
3.3.1.2.4	<i>Activity Diagram</i> Tampil Detail Email Terkirim	49
3.3.1.2.5	<i>Activity Diagram</i> Sync Email.....	51
3.3.1.2.6	<i>Activity Diagram</i> Tampil Email Masuk	52
3.3.1.2.7	<i>Activity Diagram</i> Tampil Detail Email Masuk.....	53
3.3.1.3	<i>Class Diagram</i>	55
3.3.1.4	<i>Sequence Diagram</i>	59
3.3.1.4.1	<i>Sequence Diagram</i> Konfigurasi Akun Email.....	59
3.3.1.4.2	<i>Sequence Diagram</i> Kirim Email.....	60
3.3.1.4.3	<i>Sequence Diagram</i> Tampil Email Terkirim	61
3.3.1.4.4	<i>Sequence Diagram</i> Tampil Detail Email Terkirim	62
3.3.1.4.5	<i>Sequence Diagram</i> Sync Email	63
3.3.1.4.6	<i>Sequence Diagram</i> Tampil Email Masuk	64
3.3.1.4.7	<i>Sequence Diagram</i> Tampil Detail Email Masuk	65

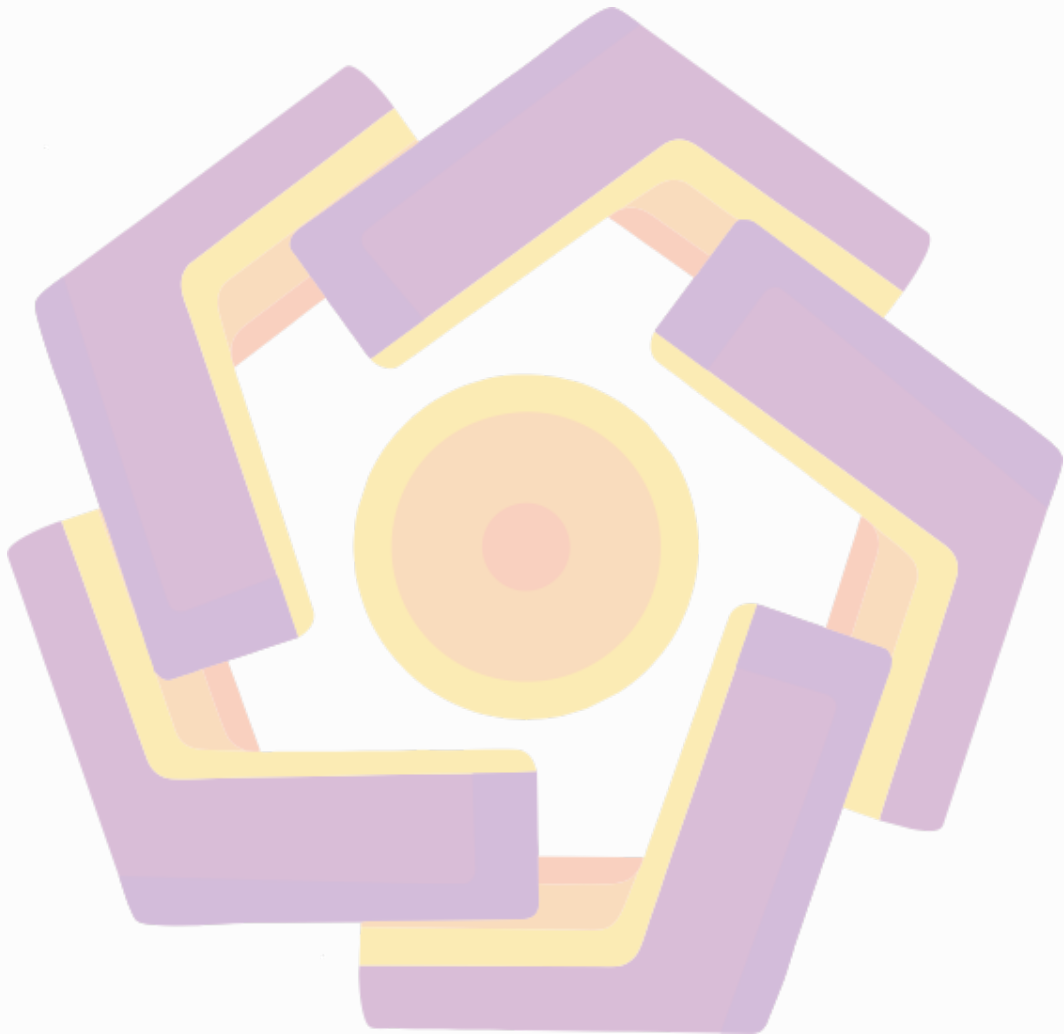
3.3.2	Struktur Aplikasi	66
3.3.3	User Interface	66
3.3.3.1	Rancangan Tampilan <i>Sign Up</i>	66
3.3.3.2	Rancangan Tampilan <i>Login</i>	67
3.3.3.3	Rancangan Tampilan <i>Create Email</i>	69
3.3.3.4	Rancangan Tampilan <i>Inbox</i>	70
3.3.3.5	Rancangan Tampilan <i>Detail Email</i>	71
3.3.3.6	Rancangan Tampilan <i>Inbox</i>	72
3.3.3.7	Rancangan Tampilan <i>Detail Email</i>	73
3.3.3.8	Rancangan Tampilan <i>Edit Profile</i>	74
BAB IV IMPLEMENTASI DAN PEMBAHASAN		75
4.1	PENYIMPANAN DATA	75
4.1.1	<i>Data User</i>	75
4.1.2	<i>Data Konfigurasi Email</i>	75
4.1.3	<i>Data Email Masuk</i>	76
4.1.4	<i>Data Email Terkirim</i>	76
4.2	USER INTERFACE	77
4.2.1	<i>User Interface Sign Up</i>	77
4.2.2	<i>User Interface Login</i>	78
4.2.3	<i>User Interface Edit Profile</i>	79
4.2.4	<i>User Interface Compose Email</i>	80
4.2.5	<i>User Interface Inbox</i>	81
4.2.6	<i>User Interface Sent Email</i>	82
4.2.7	<i>User Interface Help</i>	84
4.3	KONEKSI FORM KE <i>EMAIL SERVER</i>	84
4.3.1	Koneksi ke <i>Google Mail Server</i>	85
4.3.2	Koneksi ke <i>Yahoo Mail Server</i>	85
4.3.3	Koneksi ke <i>Outlook Mail Server</i>	86
4.4	PEMBAHASAN KODE PROGRAM	86
4.4.1	Algoritma <i>RSA</i>	86
4.4.1.1	Algoritma <i>Enkripsi RSA</i>	86

4.4.1.2	Algoritma Dekripsi RSA.....	87
4.4.2	Algoritma AES.....	88
4.4.2.1	Algoritma Enkripsi AES.....	88
4.4.2.2	Algoritma Dekripsi AES.....	89
4.5	<i>WHITE-BOX TESTING</i>	89
4.5.1	Pengujian Class User.....	89
4.5.2	Pengujian Class Email.....	92
4.6	<i>BLACK-BOX TESTING</i>	94
4.6.1	Pengujian Fitur Pendaftaran.....	94
4.6.2	Pengujian Fitur Login.....	97
4.6.3	Pengujian Fitur Kirim Email.....	97
4.6.4	Pengujian Fitur Lihat Email Masuk.....	105
4.6.5	Pengujian Fitur Lihat Email Terkirim.....	111
4.6.6	Pengujian Fitur Lihat Detail Email.....	115
4.6.7	Pengujian Fitur Update Profile.....	118
4.6.8	Pengujian Fitur Help.....	121
BAB V PENUTUP		122
5.1	KESIMPULAN.....	122
5.2	SARAN.....	123
DAFTAR PUSTAKA		124

DAFTAR TABEL

Tabel 2.1 Tabel Literatur	11
Tabel 2.2 Tabel perbandingan panjang kunci dan jumlah ronde AES	21
Tabel 2.3 Simbol-simbol <i>use case diagram</i>	25
Tabel 2.4 Simbol-simbol <i>activity diagram</i>	27
Tabel 2.5 Simbol-simbol <i>class diagram</i>	30
Tabel 2.6 Simbol-simbol <i>sequence diagram</i>	32
Tabel 3.1 Tabel Kebutuhan Fungsional, Aktor dan <i>Use Case</i> pada <i>CryptMail</i>	43
Tabel 3.2 Tabel <i>Activity</i> pada <i>Use Case</i> Konfigurasi Akun <i>Email</i>	45
Tabel 3.3 Tabel <i>activity</i> pada <i>use case</i> kirim <i>email</i>	46
Tabel 3.4 Tabel <i>Activity</i> pada <i>Use Case</i> Lihat <i>Email</i> Terkirim	48
Tabel 3.5 Tabel <i>Activity</i> pada <i>Use Case</i> Lihat Detail <i>Email</i> Terkirim	49
Tabel 3.6 Tabel <i>Activity</i> pada <i>Use Case</i> Lihat <i>Email</i> Terkirim	51
Tabel 3.7 Tabel <i>Activity</i> pada <i>Use Case</i> Lihat <i>Email</i> Masuk.....	52
Tabel 3.8 Tabel <i>Activity</i> pada <i>Use Case</i> Lihat Detail <i>Email</i> Masuk	53
Tabel 3.9 Tabel Kandidat Class Kebutuhan Fungsional 1.....	55
Tabel 3.10 Tabel Kandidat Class Kebutuhan Fungsional 2.....	55
Tabel 3.11 Tabel Kandidat Class Kebutuhan Fungsional 3.....	55
Tabel 3.12 Tabel Kandidat Class Kebutuhan Fungsional 4.....	56
Tabel 3.13 Tabel Kandidat Class Kebutuhan Fungsional 5.....	56
Tabel 3.14 Tabel Kandidat Class Kebutuhan Fungsional 6.....	56
Tabel 3.15 Tabel kandidat class pada kebutuhan fungsional 7.....	57
Tabel 4.1 Tabel hasil pengujian <i>class user</i>	90
Tabel 4.2 Tabel hasil pengujian <i>class email</i>	92
Tabel 4.3 Tabel hasil pengujian fitur pendaftaran.....	95
Tabel 4.4 Tabel hasil pengujian fitur pendaftaran.....	97
Tabel 4.5 Tabel hasil pengujian fitur kirim email	98
Tabel 4.6 Tabel hasil pengujian waktu pengiriman email	104
Tabel 4.7 Tabel hasil pengujian fitur lihat email masuk	105

Tabel 4.8 Tabel hasil pengujian waktu sinkronisasi email	111
Tabel 4.9 Tabel hasil pengujian fitur lihat email terkirim	111
Tabel 4.10 Tabel hasil pengujian fitur detail email terkirim.....	115
Tabel 4.11 Tabel hasil pengujian fitur <i>update profile</i>	119
Tabel 4.12 Tabel hasil pengujian fitur <i>help</i>	121

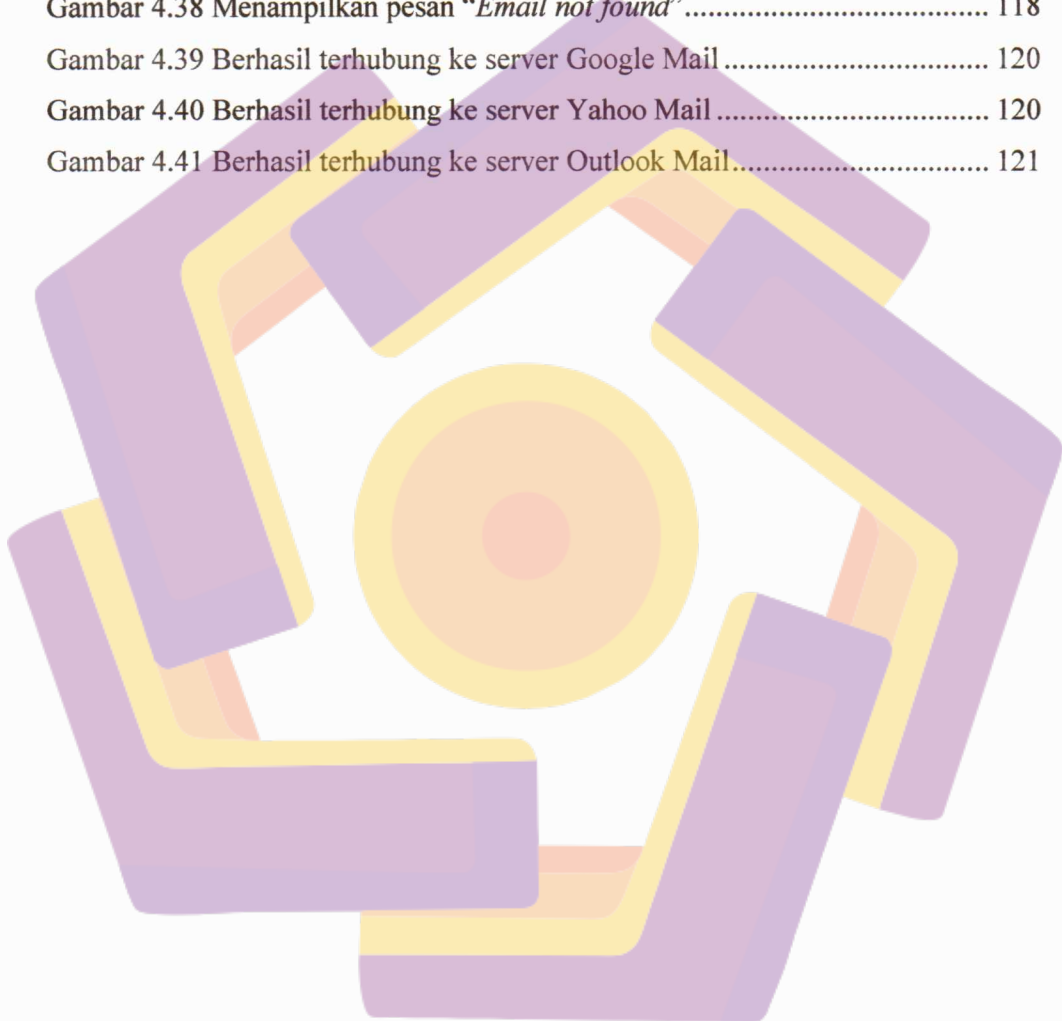


DAFTAR GAMBAR

Gambar 2.1 Ilustrasi struktur elemen sebuah dokumen XML	22
Gambar 2.2 Diagram UML	24
Gambar 2.3 Ilustrasi model <i>waterfall</i>	37
Gambar 3.1 <i>Use Case Diagram</i> Aplikasi <i>CryptMail</i>	44
Gambar 3.2 <i>Activity Diagram</i> Konfigurasi Akun <i>Email</i>	46
Gambar 3.3 <i>Activity Diagram</i> Kirim Email	47
Gambar 3.4 <i>Activity diagram</i> tampil email terkirim.....	48
Gambar 3.5 <i>Activity diagram</i> tampil email terkirim	50
Gambar 3.6 <i>Activity Diagram</i> Kirim Email	52
Gambar 3.7 <i>Activity Diagram</i> Lihat Inbox Email	53
Gambar 3.8 <i>Activity Diagram</i> Lihat Detail Email	54
Gambar 3.9 <i>Class Diagram</i>	58
Gambar 3.10 <i>Sequence diagram</i> konfigurasi akun email	59
Gambar 3.11 <i>Sequence diagram</i> kirim email.....	60
Gambar 3.12 <i>Sequence diagram</i> tampil email terkirim.....	61
Gambar 3.13 <i>Sequence diagram</i> tampil detail email terkirim	62
Gambar 3.14 <i>Sequence diagram</i> sync email	63
Gambar 3.15 <i>Sequence diagram</i> tampil email masuk	64
Gambar 3.16 <i>Sequence diagram</i> tampil detail email masuk.....	65
Gambar 3.17 Struktur Aplikasi	66
Gambar 3.18 Rancangan Tampilan <i>Sign Up</i>	67
Gambar 3.19 Rancangan Tampilan <i>Login</i>	68
Gambar 3.20 Rancangan Tampilan <i>Create Email</i>	69
Gambar 3.21 Rancangan Tampilan <i>Inbox</i>	70
Gambar 3.22 Rancangan Tampilan <i>Detail Email</i>	71
Gambar 3.23 Rancangan Tampilan <i>Inbox</i>	72
Gambar 3.24 Rancangan Tampilan <i>Detail Email</i>	73
Gambar 3.25 Rancangan Tampilan <i>Edit Profile</i>	74

Gambar 4.1 <i>User interface sign up</i>	77
Gambar 4.2 <i>User interface login</i>	78
Gambar 4.3 <i>User interface edit profile</i>	79
Gambar 4.4 <i>User interface compose email</i>	80
Gambar 4.5 <i>Tampilan file attachment</i>	80
Gambar 4.6 <i>Tampilan delete confirmation</i>	81
Gambar 4.7 <i>User interface inbox</i>	81
Gambar 4.8 <i>Tampilan detail email masuk</i>	82
Gambar 4.9 <i>User interface sent email</i>	83
Gambar 4.10 <i>Tampilan detail email masuk</i>	83
Gambar 4.11 <i>User interface help</i>	84
Gambar 4.12 <i>Pengiriman email melalui server gmail</i>	100
Gambar 4.13 <i>Hasil pengiriman email enkripsi melalui server gmail</i>	100
Gambar 4.14 <i>Hasil pengiriman email normal melalui server gmail</i>	101
Gambar 4.15 <i>Pengiriman email melalui Yahoo! Mail</i>	101
Gambar 4.16 <i>Hasil pengiriman email enkripsi melalui server Yahoo! Mail</i>	102
Gambar 4.17 <i>Hasil pengiriman email normal melalui server Yahoo! Mail</i>	102
Gambar 4.18 <i>Pengiriman email melalui server outlook mail</i>	103
Gambar 4.19 <i>Hasil pengiriman email enkripsi melalui server Outlook mail</i>	103
Gambar 4.20 <i>Hasil pengiriman email normal melalui server Outlook mail</i>	104
Gambar 4.21 <i>Menampilkan semua email masuk dari Google Mail Server</i>	107
Gambar 4.22 <i>Menampilkan semua email masuk dari Yahoo! Mail Server</i>	107
Gambar 4.23 <i>Menampilkan semua email masuk dari Outlook Mail Server</i>	108
Gambar 4.24 <i>Hasil pencarian data email berdasarkan Email Normal</i>	108
Gambar 4.25 <i>Hasil pencarian data email berdasarkan Email Enkripsi</i>	109
Gambar 4.26 <i>Hasil pencarian data email berdasarkan isi email</i>	109
Gambar 4.27 <i>Hasil pencarian data email berdasarkan pengirim email</i>	110
Gambar 4.28 <i>Hasil pencarian data email berdasarkan subject email</i>	110
Gambar 4.29 <i>Menampilkan semua email terkirim</i>	112
Gambar 4.30 <i>Hasil pencarian data email berdasarkan Email Normal</i>	113
Gambar 4.31 <i>Hasil pencarian data email berdasarkan Email Enkripsi</i>	113

Gambar 4.32 Hasil pencarian data email berdasarkan isi email	114
Gambar 4.33 Hasil pencarian data email berdasarkan penerima email.....	114
Gambar 4.34 Hasil pencarian data email berdasarkan subject email	115
Gambar 4.35 Menampilkan data detail email masuk	117
Gambar 4.36 Menampilkan pesan “ <i>Email not found</i> ”	117
Gambar 4.37 Menampilkan data detail email terkirim	118
Gambar 4.38 Menampilkan pesan “ <i>Email not found</i> ”	118
Gambar 4.39 Berhasil terhubung ke server Google Mail	120
Gambar 4.40 Berhasil terhubung ke server Yahoo Mail	120
Gambar 4.41 Berhasil terhubung ke server Outlook Mail.....	121



INTISARI

E-mail atau *electronic mail* merupakan suatu layanan yang digunakan oleh setiap orang di masa kini untuk bertukar informasi dengan orang lain. Informasi tersebut dapat berupa pesan, tulisan, gambar, suara, maupun file dokumen lainnya. Informasi-informasi yang akan dikirimkan pasti ada suatu informasi penting yang tidak ingin diketahui oleh orang selain penerima pesan tersebut. Meskipun dengan tingginya sistem keamanan yang digunakan pada layanan email pasti ada kemungkinan informasi-informasi penting tersebut terkena suatu penyadapan atau pembajakan dari pihak yang tidak bertanggungjawab.

Oleh karena itu diperlukan suatu metode pengamanan data didalam aplikasi email yang dapat digunakan untuk menyandikan informasi tersebut menjadi suatu informasi yang sangat sulit untuk dimengerti oleh pihak lain selain penerima pesan tersebut. Dengan diimplementasikannya ilmu kriptografi didalam aplikasi email pada penulisan skripsi ini, informasi-informasi yang akan dikirimkan ke server layanan email akan dienkripsi, sehingga pihak luar yang tidak memiliki aplikasi email yang tidak sama dengan pengirim email akan sangat sulit untuk membaca informasi yang ada didalam email tersebut.

Metode atau algoritma kriptografi yang akan digunakan pada penulisan skripsi ini merupakan pengkombinasian dua algoritma kriptografi modern tingkat tinggi yaitu algoritma RSA dan AES. Algoritma RSA dan AES sama-sama menggunakan kunci yang berbeda dalam melakukan enkripsi dan dekripsi pesan yang dinamakan dengan kunci privat dan kunci public. Dengan menggunakan dua kunci yang berbeda untuk melakukan enkripsi dan dekripsi, maka proses untuk kriptanalisis atau pembongkaran dan pembajakan informasi juga akan semakin sulit.

Kata Kunci : Email, Informasi, Keamanan, Kriptografi, RSA, AES, enkripsi, dekripsi

ABSTRACT

E-mail or electronic mail is a service used by everyone in the present to exchange information with others. Such information may be messages, text, images, sounds, or other document files. Information that will be sent there must be an important information that do not want to be known by people other than the recipient of the message. Despite the high security system used in the email service there is a possibility that the important information is subject to a tapping or hijacking from an irresponsible party.

Therefore required a method of data security in the email application that can be used to encode the information into an information that is very difficult to be understood by other parties in addition to the recipient of the message. With the implementation of cryptography in the email application on this thesis writing, the information that will be sent to the email service server will be encrypted, so that outside parties who do not have an email application that is not the same as the sender of email will be very difficult to read the information contained in the email.

The cryptographic method or algorithm that will be used in writing of this thesis is combining two modern high-level cryptographic algorithms RSA and AES algorithm. RSA and AES algorithms both use different keys to encrypt and decrypt messages called private key and public key. By using two different keys to encrypt and decrypt, the process for cryptanalysis or unloading and hijacking information will also be more difficult.

Keyword : *Email, Information, Security, Cryptography, RSA, AES, encryption, decryption*