

**APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN
ALGORITMA ADVANCED ENCRYPTION STANDARD
BERBASIS WEB**

SKRIPSI



disusun oleh

Muhammad Muslih Waskito

16.21.0949

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

**APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN
ALGORITMA ADVANCED ENCRYPTION STANDARD
BERBASIS WEB**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Muhammad Muslih Waskito

16.21.0949

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2017**

PERSETUJUAN

SKRIPSI

**APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN
ALGORITMA ADVANCED ENCRYPTION STANDARD
BERBASIS WEB**

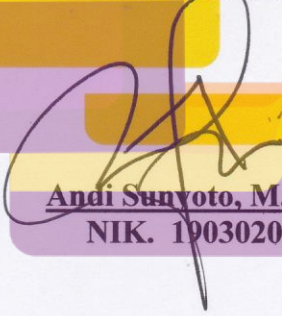
yang dipersiapkan dan disusun oleh

Muhammad Muslih Waskito

16.21.0949

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 5 Mei 2017

Dosen Pembimbing


Andi Sunyoto, M.Kom
NIK. 190302052

PENGESAHAN
SKRIPSI
APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN
ALGORITMA ADVANCED ENCRYPTION STANDARD
BERBASIS WEB

yang dipersiapkan dan disusun oleh

Muhammad Muslih Waskito

16.21.0949

telah dipertahankan didepan Dewan Penguji
pada tanggal 18 Agustus 2017

Susunan Dewan Penguji

Nama Penguji

Dony Arivus, M.Kom.
NIK. 190302128

Dina Maulina, M.Kom.
NIK. 190302250

Andi Sunyoto, M.Kom.
NIK. 190302052

Tanda Tangan

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer

tanggal 26 September 2017

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si., M.T.

NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi yang sudah dibuat merupakan karya penulis 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 penulis 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 penulis secara pribadi.

Yogyakarta, 10 September 2017



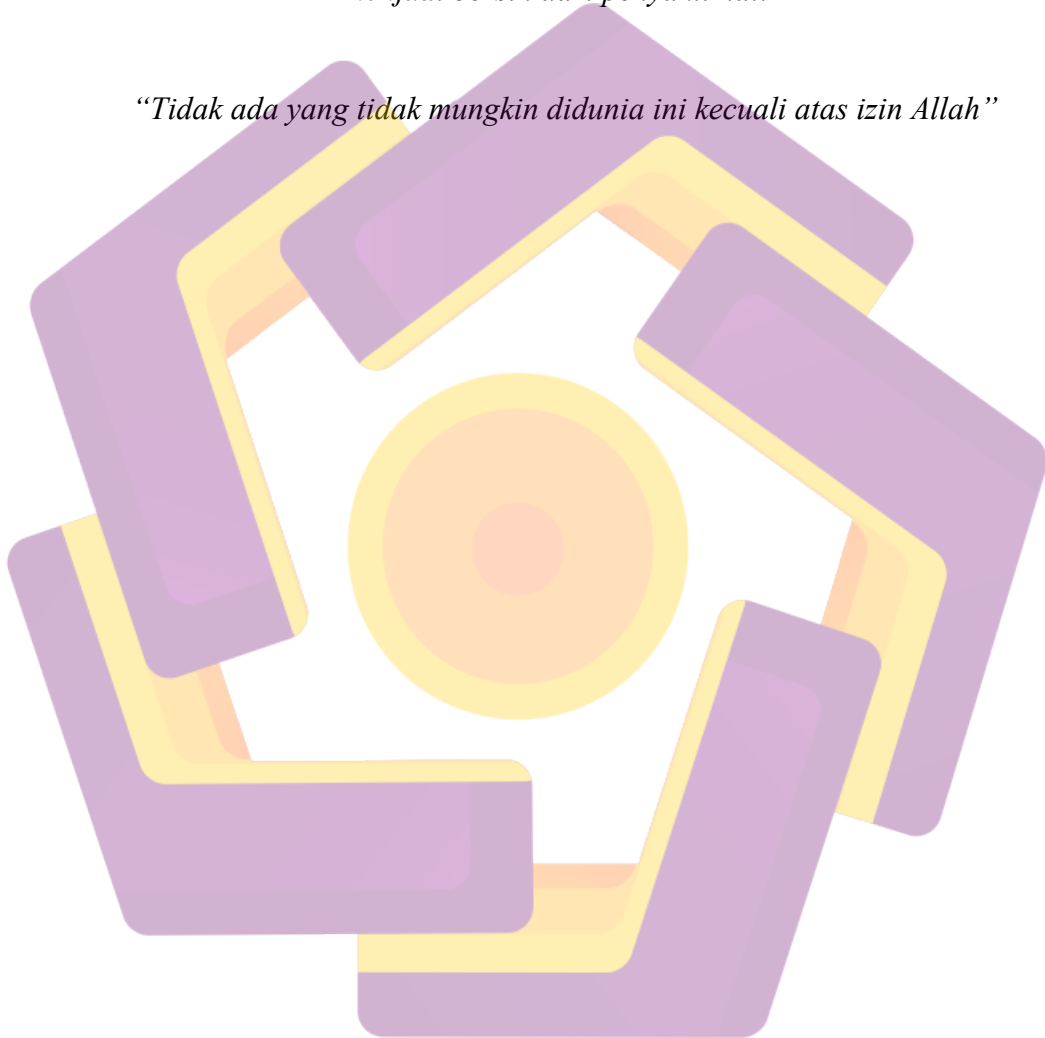
Muhammad Muslih Waskito
16.21.0949

MOTTO

“Berikhtiar dan bertawakal-lah kepada Allah maka jalanmu akan dimudahkan”

“Saling membantu satu sama lain dan berprasaangka baik akan membuat hati menjadi bersih dari penyakit hati”

“Tidak ada yang tidak mungkin didunia ini kecuali atas izin Allah”



PERSEMBAHAN

Puji syukur saya panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya, sehingga skripsi ini bisa selesai tepat waktu. Shalawat serta salam semoga tercurah kepada nabi agung Muhammad SAW beserta keluarga dan sahabat-sahabatnya. Skripsi ini saya persembahkan kepada :

1. Kedua orang tua saya dan kakak saya yang selalu mendukung, memberi semangat, motivasi serta do'a yang tanpa henti kepada saya.
2. Kepada Bapak Andi Sunyoto, M.kom dosen pembimbing terbaik dalam membimbing saya. Hanya bisa berdoa semoga bapak diberikan kemudahan dalam hidup oleh Allah SWT.
3. Spesial juga untuk Endyah Wulandari yang selalu sabar dan menyemangati saya disaat saya mengalami kekurangan motivasi dalam pengerjaan skripsi ini.
4. Sahabat dan teman-teman seperjuangan Dani, Sigit, Iqbal, Wawan, Nila, Luvi, Rita, Arlinda, Joko, Bang Andi, Arum, Retno, Leo, Mas Ridwan, Qori Alya, Alan dan semuanya Kalian luar biasa.
5. Keluarga Besar 16-SITI Transfer, Sukses buat kalian semua.
6. Untuk rekan-rekan cafe imers (Wicak, mbak Emi, mbak Nisa, mbak Alila, mas Roni dan pak Cahyo).
7. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah membantu baik dukungan moril maupun materil, pikiran, dan tenaga dalam penyelesaian Skripsi ini.

Yogyakarta, 10 September 2017

Muhammad Muslih Waskito
16.21.0949

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Alhamdulillah, dengan mengucap syukur kepada Allah SWT, atas limpahan rahmat, nikmat dan karunia-Nya serta arahan dan bimbingan dari berbagai pihak akhirnya peneliti dapat menyelesaikan penyusunan skripsi yang berjudul **“APLIKASI ENKRIPSI DAN DEKRIPSI EMAIL MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD BERBASIS WEB”**. Skripsi ini disusun sebagai salah satu persyaratan untuk menyelesaikan pendidikan pada Strata 1 dan untuk memperoleh gelar Sarjana Komputer di Universitas AMIKOM Yogyakarta.

Dalam penyusunan skripsi ini, peneliti telah menerima banyak bantuan, bimbingan serta dukungan yang sangat bermanfaat dari berbagai pihak. Oleh karena itu penulis mengucapkan terimakasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Krisnawati, S.Si, M.T selaku Ketua Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Sudarmawan, S.T, M.T selaku ketua Program Studi Informatika Universitas AMIKOM Yogyakarta.
4. Bapak Andi Sunyoto, M.Kom selaku Dosen Pembimbing, penulis berterima kasih atas bimbingan dan arahan kepada penulis dalam pembuatan skripsi.
5. Bapak dan Ibu Dosen Universitas AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama duduk di bangku perkuliahan.
6. Bapak, Ibu, Kakak dan Adik peneliti yang telah memberikan dukungan dan do'a kepada peneliti.
7. Teman-teman yang memberikan dukungan, do'a serta bantuan dalam mengerjakan skripsi.

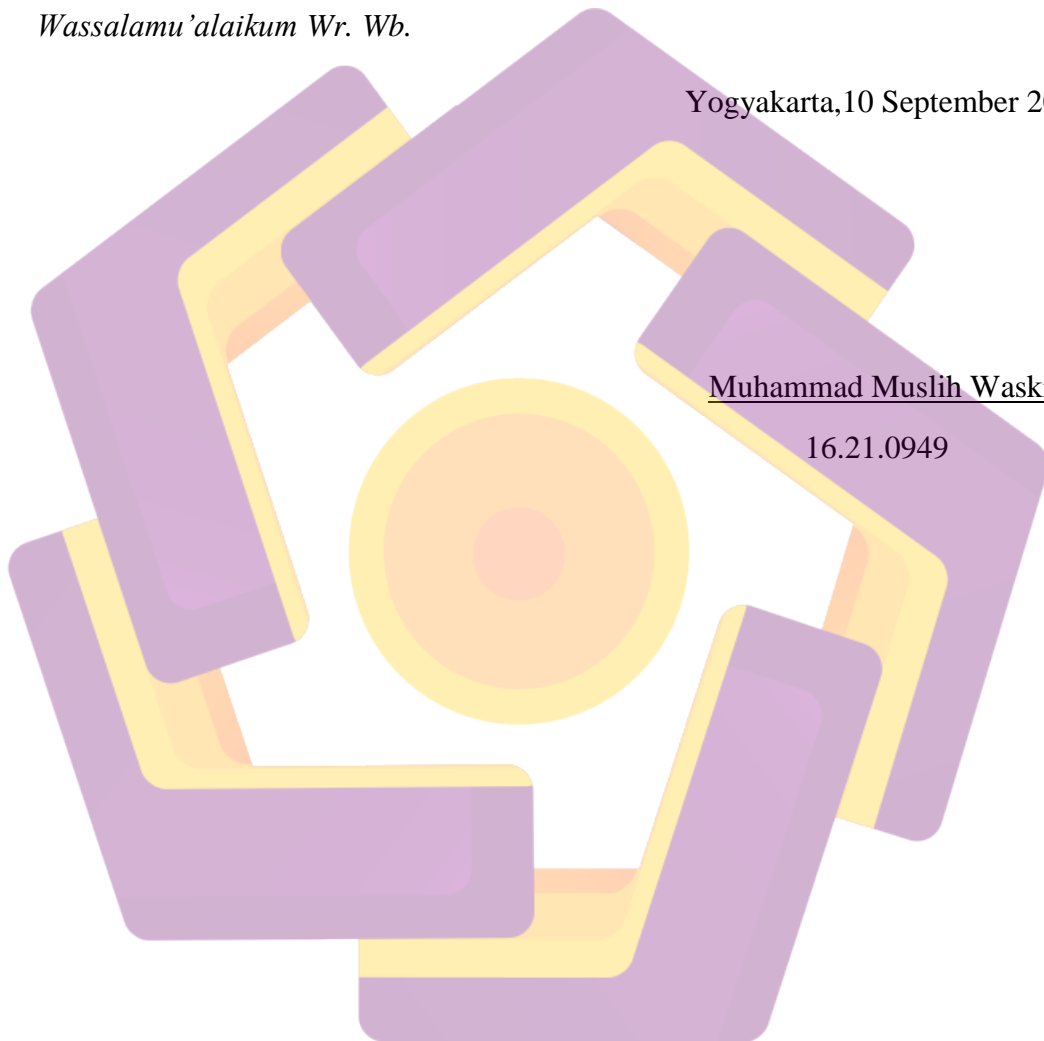
Pada akhir kata, peneliti menyadari bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan. Karena itu, peneliti berharap kepada semua pihak agar dapat menyampaikan saran dan kritik yang bersifat membangun untuk kesempurnaan skripsi ini serta semoga skripsi ini bermanfaat bagi semua pihak yang membacanya.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 10 September 2017

Muhammad Muslih Waskito

16.21.0949



DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN	iv
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
INTISARI.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Maksud dan tujuan penelitian.....	4
1.4.1 Internal	4
1.4.2 Eksternal.....	5
1.5 Manfaat Penelitian	5
1.6 Metode Penelitian	6
1.6.1 Metode Studi Kepustakaan.....	6
1.6.1.1 Metode Studi Kepustakaan	6
1.6.1.2 Metode <i>Browsing</i>	7
1.6.2 Metode Analisis.....	7
1.6.2.1 Analisis SWOT	7
1.6.2.2 Analisis Kebutuhan Sistem.....	7
1.6.2.3 Analisis Kelayakan Sistem	7
1.6.3 Metode Perancangan	7

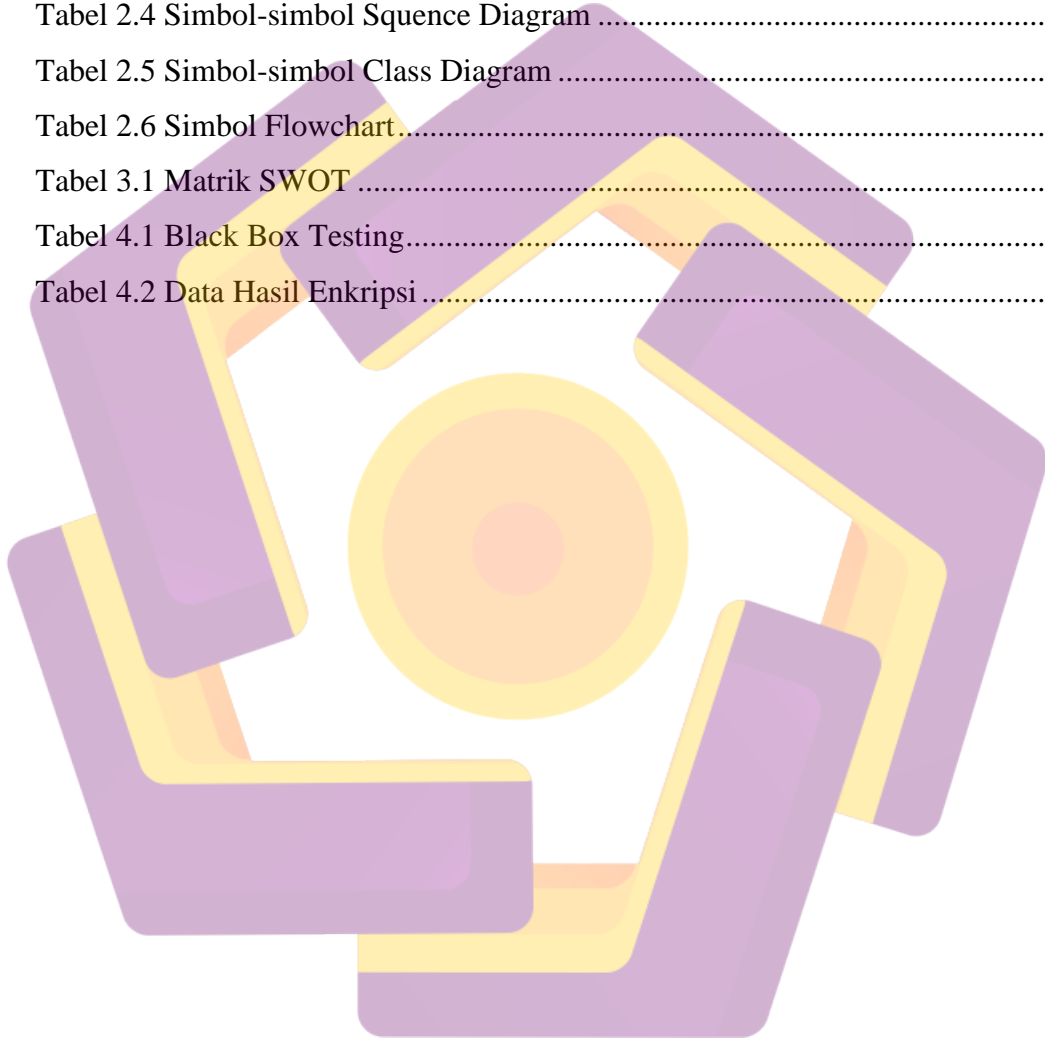
1.7 Sistematika Penulisan	8
BAB II LANDASAN TEORI	10
2.1 Tinjauan Pustaka.....	10
2.2 Kriptografi	11
2.2.1 Sejarah Kriptografi.....	11
2.2.2 Pengertian Kriptografi.....	11
2.2.3 Tujuan Kriptografi.....	12
2.2.4 Komponen Sistem Kriptografi	13
2.3 Jenis Algoritma Kriptografi.....	15
2.4 AES.....	16
2.4.1 Parameter AES.....	16
2.4.2 Proses Enkripsi AES	17
2.4.3 Proses Dekripsi AES	17
2.5 <i>Email</i>	17
2.5.1 Kelebihan Email.....	18
2.5.2 Cara Kerja Email.....	19
2.5.3 Simple Mail Transfer Protocol (SMTP).....	20
2.5.4 Post Office Protocol version 3 (POP3)	20
2.6 <i>File Document</i>	21
2.6.1 Sejarah <i>Microsoft Office</i>	21
2.7 Konsep Dasar Website.....	22
2.7.1 Pengertian WEB.....	22
2.7.2 Web Statis dan Web Dinamis.....	23
2.7.3 Perkembangan Web.....	23
2.7.4 HTML.....	24
2.7.5 CSS.....	25
2.7.6 PHP.....	25
2.7.7 MySQL.....	26
2.8 UML (<i>Unified Modeling Language</i>)	29
2.8.1 Pengenalan UML.....	29
2.8.2 Konsep Dasar UML	29

2.9 Bagan Alur (<i>flowchart</i>).....	33
2.10 Metode SWOT.....	34
2.10.1 Kekuatan.....	35
2.10.2 Kelemahan.....	35
2.10.3 Peluang.....	35
2.10.4 Ancaman.....	36
BAB III ANALISIS DAN PERANCANGAN	37
3.1 Gambaran Umum Aplikasi	37
3.2 Kelemahan Sistem Lama	39
3.3 Model Aplikasi Baru.....	39
3.4 Anallisis SWOT.....	40
3.4.1 Kekuatan (<i>Strengths</i>).....	40
3.4.2 Kelemahan (<i>Weakness</i>)	40
3.4.3 Peluang (<i>Opportunities</i>).....	41
3.4.4 Ancaman (<i>Threats</i>).....	41
3.5 Analisis Kebutuhan Sistem.....	42
3.5.1 Analisi Kebutuhan Fungsional	42
3.5.2 Analisis Kebutuhan Non-Fungsional	43
3.5.2.1 Analisis Kebutuhan Perangkat Keras (<i>Hardware</i>).....	43
3.5.2.2 Analisis Kebutuhan Perangkat Lunak (<i>Software</i>)	44
3.5.3 Analisis Kelayakan Sistem.....	44
3.5.3.1 Kelayakan Teknis	45
3.5.3.2 Kelayakan Operasional.....	45
3.6 Perancangan Sistem	45
3.6.1 Perancangan <i>Flowchart</i>	45
3.6.1.1 <i>Flowchart</i> Halaman Awal (Login dan Registrasi).....	46
3.6.1.2 <i>Flowchart</i> Tulis Pesan dan Enkripsi Pesan	46
3.6.1.3 <i>Flowchart</i> Pesan Masuk dan Dekripsi Pesan.....	47
3.6.1.4 <i>Flowchart</i> Enkripsi dan Dekripsi File	48
3.6.2 Perancangan UML.....	48
3.6.2.1 Use Case Diagram	49

3.6.2.2 Activity Diagram	49
3.6.2.3 Class Diagram.....	55
3.6.2.4 Sequence Diagram	56
3.6.3 Perancangan Interface Aplikasi Enkripsi <i>Email</i>	61
3.6.3.1 Rancangan Interface Halaman Login	61
3.6.3.2 Rancangan Interface Halaman Register.....	62
3.6.3.3 Rancangan Interface Halaman User Profile.....	62
3.6.3.4 Rancangan Interface Halaman Tulis Pesan	62
3.6.3.5 Rancangan Interface Halaman Kotak Masuk	63
3.6.3.6 Rancangan Interface Halaman Detail Pesan.....	63
3.6.3.7 Rancangan Interface Halaman Enkripsi File	64
3.6.3.8 Rancangan Interface Halaman Dekripsi File.....	64
BAB IV IMPLEMENTASI DAN PEMBAHASAN	66
4.1 Implementasi Program	66
4.1.1 Halaman <i>Login</i>	66
4.1.2 Halaman Register	68
4.1.3 Halaman <i>User Profile</i>	70
4.1.4 Halaman Tulis Pesan.....	70
4.1.5 Halaman Kotak Masuk.....	73
4.1.6 Halaman Detail Pesan	74
4.1.7 Halaman Enkripsi <i>File</i>	76
4.1.8 Halaman Dekripsi <i>File</i>	77
4.2 Pengujian Sistem.....	79
4.2.1 <i>White Box Testing</i>	79
4.2.2 <i>Black Box Testing</i>	81
BAB V PENUTUP.....	83
5.1 Kesimpulan	83
5.2 Saran.....	83
Daftar Pustaka	85

DAFTAR TABEL

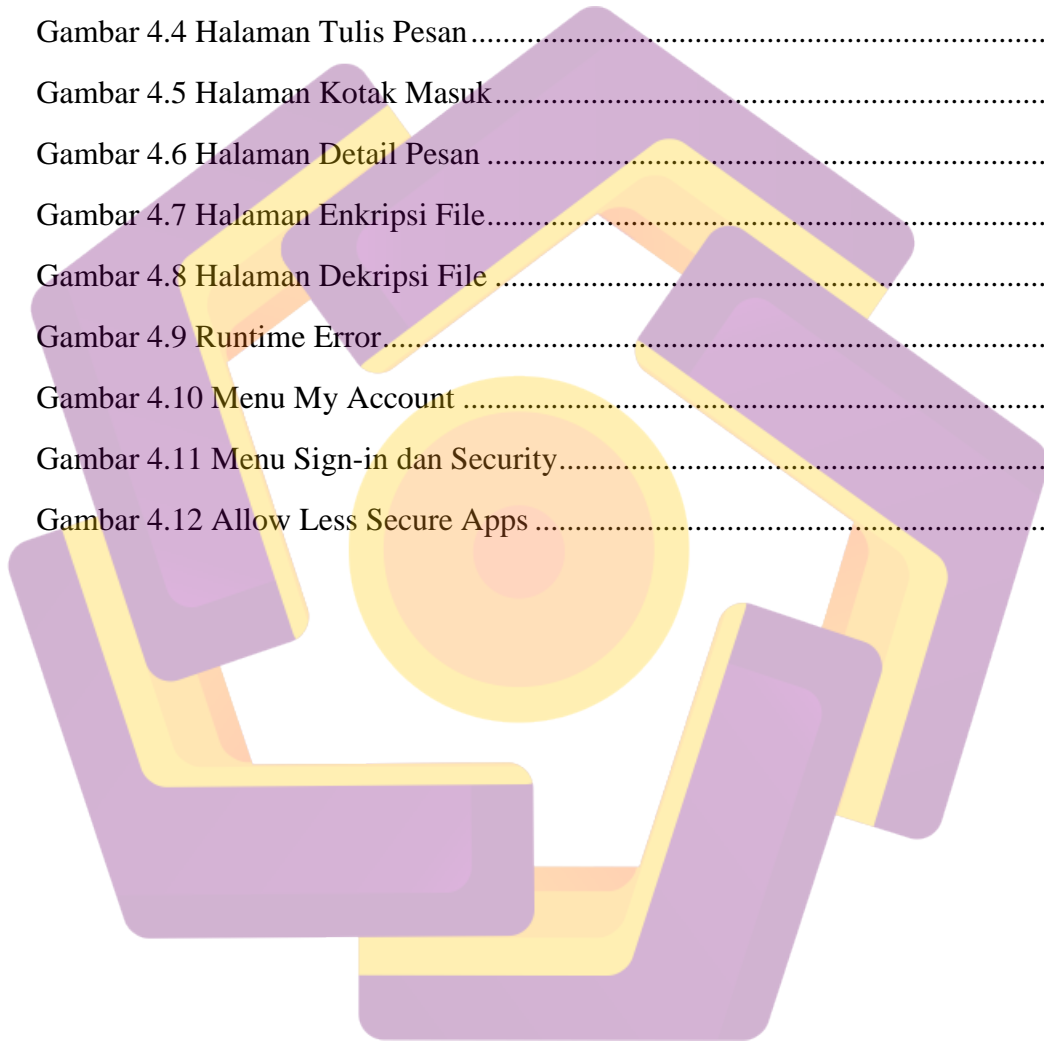
Table 2.1 Parameter AES	16
Tabel 2.2 Simbol-simbol Use Case Diagram	29
Tabel 2.3 Simbol-simbol Activity Diagram	31
Tabel 2.4 Simbol-simbol Squence Diagram	31
Tabel 2.5 Simbol-simbol Class Diagram	32
Tabel 2.6 Simbol Flowchart	33
Tabel 3.1 Matrik SWOT	41
Tabel 4.1 Black Box Testing	81
Tabel 4.2 Data Hasil Enkripsi	82



DAFTAR GAMBAR

Gambar 3.1 Sistem Penerimaan <i>Email</i> Tanpa Kriptografi.....	38	
Gambar 3.2 Sistem Pengiriman Email Menggunakan Kriptografi	38	
Gambar 3.3 Flowchart Halaman Utama (Login dan Registrasi akun).....	46	
Gambar 3.4 Flowchart Tulis Pesan dan Enkripsi Pesan	47	
Gambar 3.5 Flowchart Pesan Masuk dan Dekripsi Pesan.....	47	
Gambar 3.6 Flowchart Enkripsi dan Dekripsi File	48	
Gambar 3.7 Use Case Diagram	Gambar 3.8 Activity Diagram Register.....	49
Gambar 3.8 Activity Diagram Register	50	
Gambar 3.9 Activity Diagram Login	51	
Gambar 3.10 Activity Diagram Tulis Pesan	52	
Gambar 3.11 Activity Diagram Pesan Masuk.....	53	
Gambar 3.12 Activity Diagram Enkripsi File	54	
Gambar 3.13 Activity Diagram Dekripsi File.....	55	
Gambar 3.14 Class Diagram	56	
Gambar 3.15 Squence Diagram Register	57	
Gambar 3.16 Squence Diagram Login.....	58	
Gambar 3.17 Squence Diagram Tulis/Kirim Pesan Email.....	59	
Gambar 3.18 Squence Diagram Pesan Masuk	59	
Gambar 3.19 Squence Diagram Enkripsi File.....	60	
Gambar 3.20 Squence Diagram Dekripsi File	61	
Gambar 3.21 Rancangan Interface Halaman Login	61	
Gambar 3.22 Rancangan Interface Halaman Register	62	
Gambar 3.23 Rancangan Interface Halaman Login	62	
Gambar 3.24 Rancangan Interface Halaman Tulis Pesan	63	
Gambar 3.25 Rancangan Interface Halaman Kotak Masuk.....	63	
Gambar 3.26 Rancangan Interface Halaman Detail Pesan	64	

Gambar 3.27 Rancangan Interface Halaman Enkripsi File.....	64
Gambar 3.28 Rancangan Interface Halaman Dekripsi File	65
Gambar 4.1 Halaman Login.....	67
Gambar 4.2 Halaman Register	69
Gambar 4.3 Halaman User Profile	70
Gambar 4.4 Halaman Tulis Pesan.....	71
Gambar 4.5 Halaman Kotak Masuk.....	73
Gambar 4.6 Halaman Detail Pesan	75
Gambar 4.7 Halaman Enkripsi File.....	76
Gambar 4.8 Halaman Dekripsi File	78
Gambar 4.9 Runtime Error.....	79
Gambar 4.10 Menu My Account	80
Gambar 4.11 Menu Sign-in dan Security.....	80
Gambar 4.12 Allow Less Secure Apps	81



INTISARI

Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (message). Kriptografi telah banyak diimplementasikan di banyak hal seperti Smart card, Anjungan Tunai Mandiri (ATM), Pay TV, Mobile Phone, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya. Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibaca manusia (plainteks) ke bentuk lain yang tidak dapat dimengerti/dibaca oleh manusia (cipherteks). Proses transformasi plainteks menjadi cipherteks diistilahkan dengan enkripsi. Sedang proses pengembalian pesan cipherteks menjadi plainteks diistilahkan dengan dekripsi.

Ada banyak algoritma kriptografi, dalam penelitian ini aplikasi kriptografi yang dikembangkan untuk enkripsi dan dekripsi email menggunakan algoritma simetri AES (Advanced Encryption Standard) dengan menggunakan bahasa pemrograman PHP, HTML dan CSS. Advanced Encryption Standard (AES) merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 and AES-256.

Aplikasi ini dibuat dengan menggunakan program sublime text untuk pembuatan interface dan sistem aplikasinya, XAMPP sebagai virtualserver dan MySql sebagai penyimpan data (database). Dalam pengujiannya, Aplikasi Enkripsi dan Dekripsi Email ini mampu melindungi data yang dikirim oleh pengguna melalui pesan email.

Kata Kunci : *Plainteks, Cipherteks, Kriptografi, Advanced Encryption Standard (AES), sublimetext, MySql, XAMPP*

ABSTRACT

Abstract – Cryptography is the field of science to maintain the security of messages (message). Cryptography has been widely implemented in many ways such as Smart cards, Automated Teller Machines (ATMs), Pay TV, Mobile Phones, and Computers are some examples of technology products that use cryptography for security. The way it works is by changing the original message that a human can understand / read (plaintext) into another form that can not be understood / read by humans (cipherteks). The process of plaintext transformation into chiperteks is termed encryption. While the process of returning a text message into text is plaintext termed with decryption.

There are many cryptographic algorithms, in this research cryographic application developed for encryption and email decryption using AES (Advanced Encryption Standard) symmetry algorithm using PHP, HTML and CSS programming languages. Advanced Encryption Standard (AES) is a key-symmetric encryption standard adopted by the United States government. This standard consists of 3 blocks of ciphers, namely AES-128, AES-192 and AES-256.

This application is created by using sublime text program to pembuatan interface and application system, XAMPP as virtualserver and MySql as data storage (database). In testing, the Email Encryption and Decryption application is able to protect data sent by users via email messages.

Keywords: Plaintext, Ciphertext, Cryptography, Advanced Encryption Standard (AES), sublimetext, MySql, XAMPP