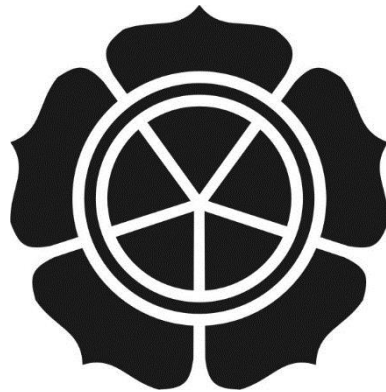


**ENKRIPSI GAMBAR MENGGUNAKAN METODE
STEGANOGRAFI LSB BERBASIS WEBSITE**

SKRIPSI



disusun oleh

Amri Arifin Hidayat

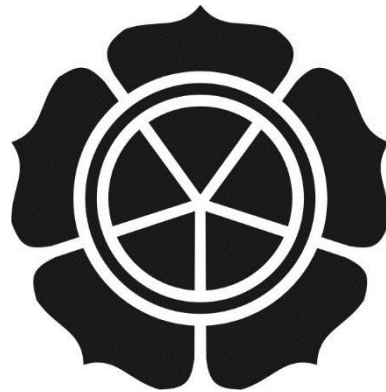
11.11.5536

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

**ENKRIPSI GAMBAR MENGGUNAKAN METODE
STEGANOGRAFI LSB BERBASIS WEBSITE**

SKRIPSI

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



disusun oleh

Amri Arifin Hidayat

11.11.5536

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

PERSETUJUAN

SKRIPSI

**ENKRIPSI GAMBAR MENGGUNAKAN METODE
STEGANOGRAFI LSB BERBASIS WEBSITE**

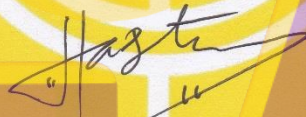
yang disusun oleh

Amri Arifin Hidayat

11.11.5536

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Oktober 2015

Dosen Pembimbing,



Hastari Utama, M.Cs
NIK. 190302230

PENGESAHAN

SKRIPSI

**ENKRIPSI GAMBAR MENGGUNAKAN METODE
STEGANOGRAFI LSB BERBASIS WEBSITE**

yang disusun oleh
Amri Arifin Hidayat

11.11.5536

telah dipertahankan di depan Dewan Penguji
pada tanggal 19 April 2016

Susunan Dewan Penguji

Nama Penguji

Kusrini, Dr., M.Kom
NIK. 190302106

Dina Maulina, M.Kom
NIK. 190302250

Rizqi Sukma Kharisma, M.Kom
NIK. 190302215

Tanda Tangan

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
pada tanggal 1 Juni 2016

KETUA STMIK AMIKOM YOGYAKARTA

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

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, 11 Juni 2016



Amri Arifin Hidayat
NIM 11.11.5536

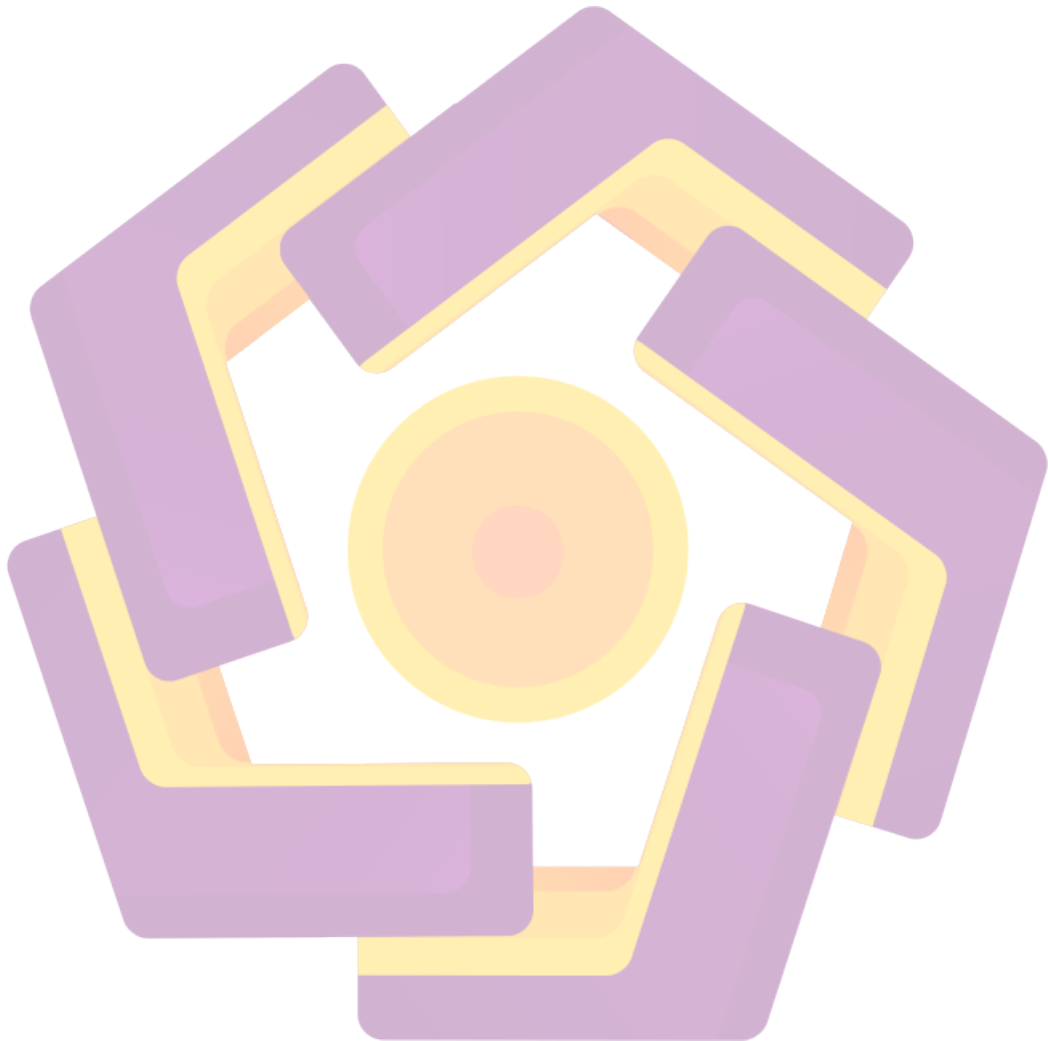
MOTTO

Jadilah sempurna.



PERSEMBAHAN

Ibu.



KATA PENGANTAR

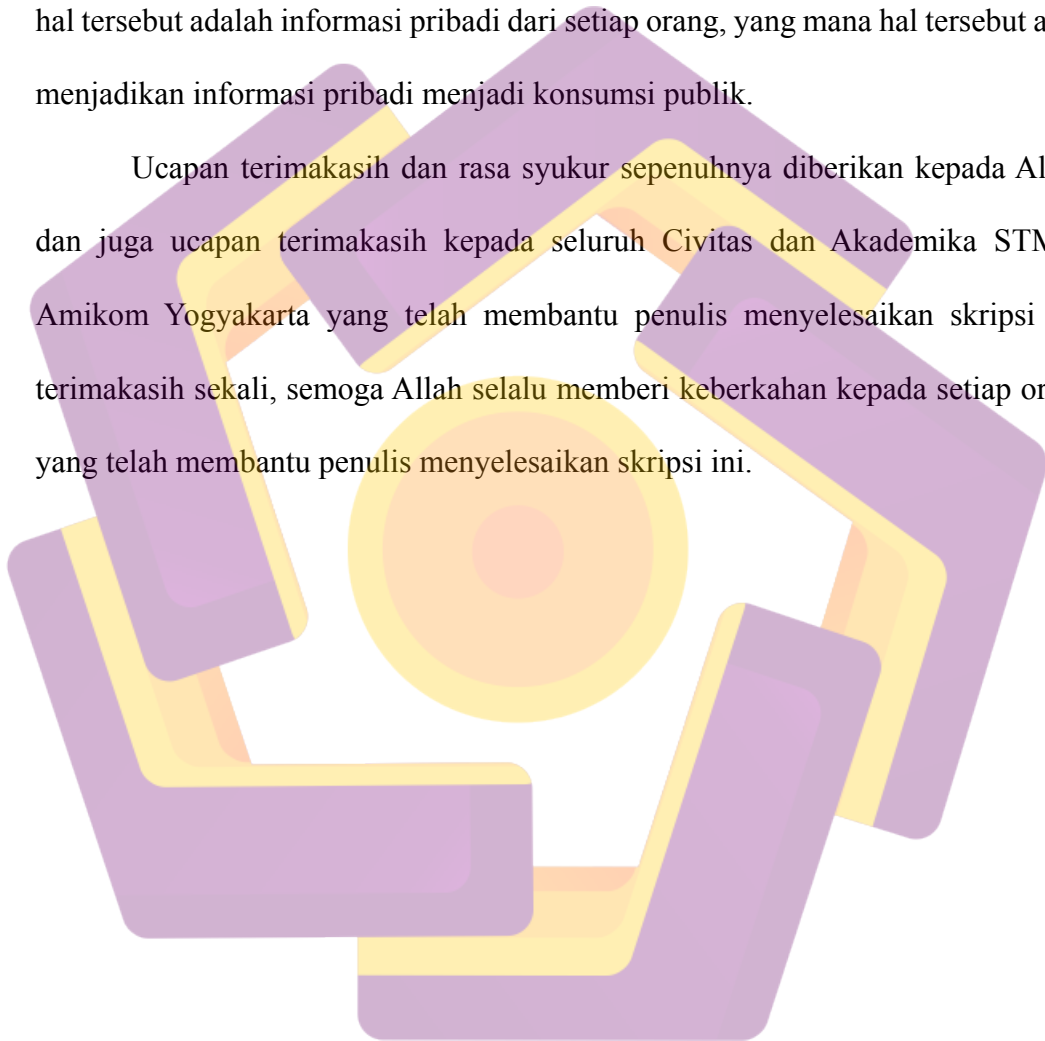
Kerahasiaan informasi di era keterbukaan seperti saat ini untuk sebagian orang sangatlah penting dan tidak mungkin untuk diabaikan begitu saja. Para pengguna alat komunikasi yang peduli terhadap keamanan dan kerahasiaan dari isi komunikasi yang dikirimkan tidak akan dengan sengaja melakukan tindakan ceroboh dalam mengirimkan sebuah informasi kepada orang lain, akan ada sebuah tindakan pencegahan sebelum mengirimkan informasi misalnya apabila informasi yang disampaikan dibaca oleh orang yang bukan penerima sesungguhnya yang dimaksud oleh pengirim informasi tersebut. Menggunakan teknik merahasiakan pesan dengan steganografi dapat menjadi satu solusi dalam tindakan pencegahan tersebut.

Kerahasiaan informasi sangat erat kaitannya dengan tindakan pengguna alat komunikasi itu sendiri dalam melindungi informasi privasinya, jika pengguna tersebut *concern* terhadap privasinya kemungkinan besar dipastikan akan berhati-hati dalam berkirim informasi dengan orang lain. Diambil contoh misal pengguna media sosial Facebook yang peduli dengan data pribadinya, pengguna ini akan dengan hati-hati dengan apa yang ditulis dalam postingannya, ataupun yang ditulis dalam bio Facebooknya, tindakan kehati-hatian ini sebagai sebuah tindakan pencegahan apabila postingan ataupun informasi di biodatanya dapat mengakibatkan masalah bagi pengguna tersebut di kemudian hari.

Tetapi jika seseorang sudah *go public* ke dunia maya, sangat mengherankan apabila berbicara mengenai privasi, karena menurut pandangan penulis, apabila seseorang sudah masuk ke dunia maya itu artinya orang tersebut secara tidak

langsung sudah siap apabila privasinya ataupun informasi pribadinya menjadi konsumsi publik. Sebagai contoh apabila seseorang akan mendaftar menjadi pengguna Facebook, dalam halaman pendaftaran pengguna akan dituntun untuk memasukkan data pribadi nama, tanggal lahir dan tempat tinggal, yang mana hal tersebut adalah informasi pribadi dari setiap orang, yang mana hal tersebut akan menjadikan informasi pribadi menjadi konsumsi publik.

Ucapan terimakasih dan rasa syukur sepenuhnya diberikan kepada Allah, dan juga ucapan terimakasih kepada seluruh Civitas dan Akademika STMIK Amikom Yogyakarta yang telah membantu penulis menyelesaikan skripsi ini, terimakasih sekali, semoga Allah selalu memberi keberkahan kepada setiap orang yang telah membantu penulis menyelesaikan skripsi ini.



DAFTAR ISI

HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN	v
HALAMAN MOTTO	vi
HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
INTISARI	xvii
ABSTRACT	xviii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	1
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	2
1.5 Manfaat Penelitian	2
1.5.1 Bagi Penulis	2
1.5.2 Bagi Pengguna.....	2
1.5.3 Bagi STMIK AMIKOM Yogyakarta	3
1.6 Metode Penelitian	3
1.6.1 Metode Pengumpulan Data	3
1.6.2 Metode Perancangan	3
1.7 Sistematika Penulisan Laporan	3
BAB II LANDASAN TEORI	5
2.1 Tinjauan Pustaka	5
2.2 Konsep Dasar Sistem	6
2.3 Konsep Dasar Informasi	7
2.4 Konsep Dasar Sistem Informasi	7

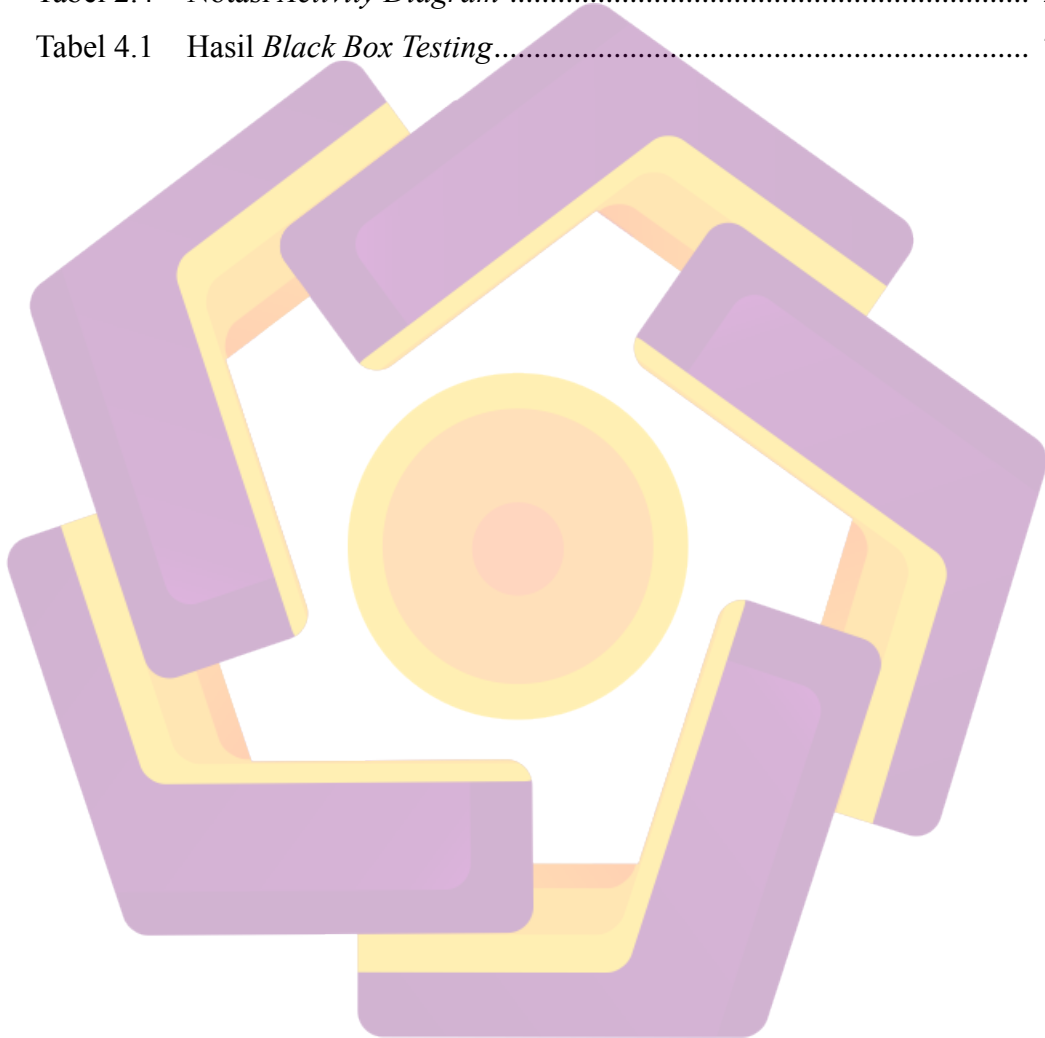
2.5	Perangkat Lunak	7
2.6	HTML5	9
2.6.1	Pengeritan HTML5	9
2.6.2	Fitur-fitur HTML5	9
2.6.2.1	<i>The Canvas</i>	9
2.6.2.2	<i>Geolocation</i>	10
2.6.2.3	<i>Audio and Video</i>	11
2.6.2.4	<i>Forms</i>	11
2.6.2.5	<i>Local Storage</i>	11
2.6.2.6	<i>Web Workers</i>	11
2.6.2.7	<i>Web Applications</i>	12
2.6.2.8	<i>Microdata</i>	12
2.7	PHP	13
2.8	Unified Modelling Language (UML)	13
2.8.1	Pengeritan UML	13
2.8.2	Diagram-diagram UML	14
2.8.2.1	<i>Use Case Diagram</i>	14
2.8.2.2	<i>Class Diagram</i>	17
2.8.2.3	<i>Sequence Diagram</i>	18
2.8.2.4	<i>Activity Diagram</i>	20
2.9	Apache Web Server	21
2.10	Kriptografi	23
2.11	Steganografi	24
2.11.1	Pengeritan Steganografi.....	24
2.11.2	Tipe-tipe Steganografi	25
2.12	Metode <i>Least Significant Bit</i>	25
2.13	Stegger	27
2.14	Enkripsi	31
2.15	Secrypt	33
2.16	Gammu	33
BAB III ANALISIS DAN PERANCANGAN SISTEM		34

3.1 Analisis Masalah	34
3.2 Solusi yang Dapat Diterapkan	34
3.3 Solusi yang Dipilih	35
3.4 Analisis Sistem	35
3.4.1 Analisis SWOT.....	35
3.4.1.1 Kekuatan.....	35
3.4.1.2 Kelemahan.....	36
3.4.1.3 Peluang	36
3.4.1.4 Ancaman.....	36
3.4.2 Analisis Kebutuhan	36
3.4.2.1 Kebutuhan Fungsional.....	37
3.4.2.2 Kebutuhan Non-Fungsional.....	37
3.4.2.2.1 Kebutuhan Perangkat Keras.....	37
3.4.2.2.2 Kebutuhan Perangkat Lunak	37
3.4.2.3 Kebutuhan Informasi	38
3.4.2.4 Kebutuhan Pengguna	38
3.5 Perancangan Aplikasi	38
3.5.1 Perancangan Proses	38
3.5.1.1 <i>Usecase Diagram</i>	39
3.5.1.2 <i>Activity Diagram</i>	39
3.5.1.3 <i>Sequence Diagram</i>	48
3.5.1.4 <i>Class Diagram</i>	51
3.5.2 Perancangan Antarmuka.....	52
3.5.2.1 Rancangan Tampilan Antarmuka Menu Enkripsi	52
3.5.2.2 Rancangan Tampilan Antarmuka Menu Dekripsi	53
3.5.2.3 Rancangan Tampilan Antarmuka Menu Privasi dan Ketentuan untuk Member dan Nonmember	54
3.5.2.4 Rancangan Tampilan Antarmuka Menu Cara Penggunaan untuk Nonmember	55
3.5.2.5 Rancangan Tampilan Antarmuka Menu Kontak untuk Nonmember	56

3.5.2.6	Rancangan Tampilan Antarmuka Menu Login.....	57
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	58
4.1	Pembuatan Tampilan Antarmuka	58
4.1.1	Tampilan Antarmuka Halaman Utama	59
4.1.2	Tampilan Halaman Privasi dan Ketentuan untuk Nonmember ...	59
4.1.3	Tampilan Halaman Cara Penggunaan untuk Nonmember	60
4.1.4	Tampilan Halaman Kontak untuk Nonmember	61
4.1.5	Tampilan Antarmuka Halaman Login	62
4.1.6	Tampilan Antarmuka Halaman Enkripsi	63
4.1.7	Tampilan Antarmuka Halaman Dekripsi	67
4.2	Pengujian Sistem	71
4.2.1	<i>White Box Testing</i>	71
4.2.2	<i>Black Box Testing</i>	73
4.3	Distribusi	75
BAB V	PENUTUP	76
5.1	Kesimpulan	76
5.2	Saran	76
DAFTAR PUSTAKA	77

DAFTAR TABEL

Tabel 2.1	Notasi <i>Use Case Diagram</i>	15
Tabel 2.2	Notasi <i>Class Diagram</i>	17
Tabel 2.3	Notasi <i>Sequence Diagram</i>	19
Tabel 2.4	Notasi <i>Activity Diagram</i>	20
Tabel 4.1	Hasil <i>Black Box Testing</i>	72



DAFTAR GAMBAR

Gambar 2.1	Contoh gambar	29
Gambar 2.2	Terdapat pixel dalam gambar	29
Gambar 2.3	Tiap pixel terdiri dari berbagai warna	30
Gambar 2.4	Tiap warna terdiri dari tiga warna primer	30
Gambar 2.5	Tiap warna primer terdiri dari nilai biner	31
Gambar 2.6	Tiap 8 pixel dapat menyimpan 3 karakter	31
Gambar 3.1	Rancangan <i>usecase diagram</i> aplikasi	39
Gambar 3.2	Rancangan <i>activity diagram</i> untuk menu Enkripsi	40
Gambar 3.3	Rancangan <i>activity diagram</i> untuk menu Dekripsi	41
Gambar 3.4	Rancangan <i>activity diagram</i> untuk menu Privasi dan Ketentuan untuk member	42
Gambar 3.5	Rancangan <i>activity diagram</i> untuk menu Privasi dan Ketentuan untuk nonmember	43
Gambar 3.6	Rancangan <i>activity diagram</i> untuk menu Cara Penggunaan untuk member	44
Gambar 3.7	Rancangan <i>activity diagram</i> untuk menu Cara Penggunaan untuk nonmember	45
Gambar 3.8	Rancangan <i>activity diagram</i> untuk menu Kontak untuk member	46
Gambar 3.9	Rancangan <i>activity diagram</i> untuk menu Kontak untuk nonmember	47
Gambar 3.10	Sequence diagram untuk registrasi	48
Gambar 3.11	Sequence diagram untuk login	49
Gambar 3.12	Sequence diagram untuk enkripsi	49
Gambar 3.13	Sequence diagram untuk dekripsi	50
Gambar 3.14	Rancangan class diagram aplikasi	51
Gambar 3.15	Rancangan antarmuka menu Enkripsi	52
Gambar 3.16	Rancangan antarmuka menu Dekripsi	53
Gambar 3.14	Rancangan antarmuka menu Privasi dan Ketentuan untuk member	

	dan nonmember	54
Gambar 3.15	Rancangan antarmuka menu Cara Penggunaan untuk member dan nonmember	55
Gambar 3.16	Rancangan antarmuka menu Kontak untuk member dan nonmember	56
Gambar 3.17	Rancangan antarmuka menu Login	57
Gambar 4.1	Alur pembuatan tampilan antarmuka dengan Artisteer	58
Gambar 4.2	Halaman utama	59
Gambar 4.3	Halaman privasi dan ketentuan untuk nonmember	59
Gambar 4.4	Halaman cara penggunaan untuk nonmember	60
Gambar 4.5	Halaman cara penggunaan enkripsi untuk nonmember	60
Gambar 4.6	Halaman cara penggunaan dekripsi untuk nonmember	61
Gambar 4.7	Halaman kontak untuk nonmember	61
Gambar 4.8	Antarmuka halaman login	62
Gambar 4.9	Halaman enkripsi tahap pertama	63
Gambar 4.10	Halaman enkripsi tahap kedua	64
Gambar 4.11	Halaman enkripsi tahap ketiga	65
Gambar 4.12	Halaman dekripsi tahap pertama	67
Gambar 4.13	Halaman dekripsi tahap kedua	68

INTISARI

Perkembangan teknologi komunikasi yang semakin maju saat ini sangat memudahkan pengguna teknologi ini untuk saling bertukar informasi dengan cepat. Semua seharusnya sudah tahu kalau sekarang teknologi kirim pesan teks dengan SMS maupun dengan layanan kirim pesan berkas MMS, sudah mulai ditinggalkan, terganti dengan aplikasi layanan *chatting* yang tersedia gratis dalam *smartphone* ataupun melalui website.

Namun bagaimana kalau pesan teks ataupun berkas yang dikirimkan melalui aplikasi *chat* yang digunakan juga dapat diterima oleh subjek yang tidak berhak menerimanya, hal ini akan benar-benar merugikan kedua belah pihak, baik pengirim maupun penerima pesan yang sah.

Salah satu jalan keluar yang dapat digunakan untuk meminimalisir tindakan merugikan diatas adalah dengan melindungi berkas ataupun pesan yang akan kita kirim dengan pengamanan menggunakan teknik kriptografi dan steganografi.

Kata kunci: steganografi, kriptografi, teknologi.



ABSTRACT

The development of increasingly advanced communications technology is now very easy for users of this technology to exchange information quickly. All should know that the technology now send SMS text messages as well as send a message with the service MMS files, are becoming obsolete, replaced by applications chat service is available for free in the smartphone or via the website.

But what if the text messages or files sent through chat applications used can also be received by the subjects who did not deserve it, it would really hurt both sides, both the sender and recipient of the message is legitimate.

One way out that can be used to minimize the adverse action to protect the file or message would we send to the security using cryptography and steganography techniques.

Keywords: steganography, cryptography, technology.

