

**APLIKASI PENGAMAN DATA DAN INFORMASI BERLAPIS DENGAN  
METODE STEGANOGRAFI LSB , KRIPTOGRAFI OPENSLL  
DAN MD5 BERBASIS WEB**

**SKRIPSI**



disusun oleh

**Achmed Robeth Muzaki**

**11.11.5362**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA  
2015**

**APLIKASI PENGAMAN DATA DAN INFORMASI BERLAPIS DENGAN  
METODE STEGANOGRAFI LSB , KRIPTOGRAFI OPENSLL  
DAN MD5 BERBASIS WEB**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai derajat Sarjana S1  
pada jurusan Sistem Informasi



disusun oleh

**Achmed Robeth Muzaki**

**11.11.5362**

**JURUSAN TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
AMIKOM YOGYAKARTA  
YOGYAKARTA  
2015**

**PERSETUJUAN**

**SKRIPSI**

**APLIKASI PENGAMAN DATA DAN INFORMASI BERLAPIS DENGAN  
METODE STEGANOGRAFI LSB , KRIPTOGRAFI OPENSLL  
DAN MD5 BERBASIS WEB**

yang disusun oleh

**Achmed Robeth Muzaki**

**11.11.5362**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 18 November 2014

Dosen Pembimbing,

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

**PENGESAHAN**

**SKRIPSI**

**APLIKASI PENGAMAN DATA DAN INFORMASI BERLAPIS DENGAN  
METODE STEGANOGRAFI LSB , KRIPTOGRAFI OPENSLL  
DAN MD5 BERBASIS WEB**

yang disusun oleh

**Achmed Robeth Muzaki**

**11.11.5362**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 15 Desember 2014

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

Armadyah Amborowati, S.Kom, M. Eng.  
NIK. 190302063

Barka Satya, M.Kom.  
NIK. 190302126

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



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 15 Desember 2014



**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, 15 Desember 2014.

Achmed Robeth Muzaki  
NIM. 11.11.5362

## MOTTO

- ✓ Bisa , karena terbiasa.
- ✓ Berani kuliah, Berani Skripsi. (Kata bapak ku)
- ✓ Kalau bukan kita siapa lagi? Kalau bukan sekarang kapan lagi?

#Skripsi

- ✓ Keberuntungan adalah sesuatu yang terjadi ketika kesempatan bertemu dengan kesiapan.
- ✓ *"An action is the foundation of a success."*
- ✓ *"The Intelligent people can lose because of the tenacity of the fools."*

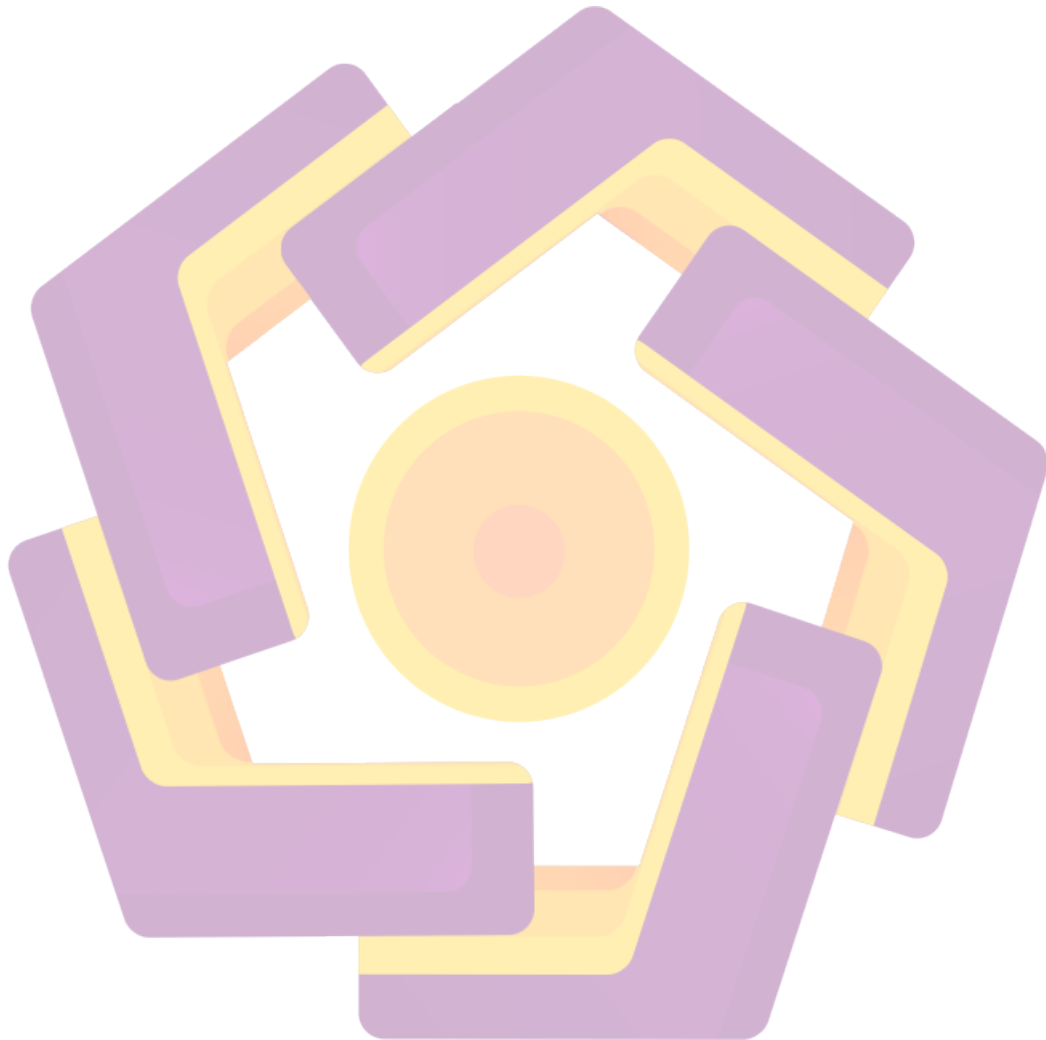
## PERSEMBAHAN

Puji syukur kepada Allah subhanahu wata'ala, atas segala nikmat hidup dan kesempatan mengenggam ilmu, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Aplikasi Pengaman Data dan Informasi Berlapis dengan Metode Steganografi LSB, Kriptografi OpenSSL dan Md5 Berbasis Web”. Skripsi ini disusun sebagai salah satu persyaratan untuk mencapai derajat Sarjana Teknik Informatika STMIK AMIKOM Yogyakarta. Dalam penelitian dan penyusunan skripsi ini, penulis banyak dibantu, dibimbing, dan didukung oleh berbagai pihak. Oleh karena itu, pada kesempatan ini penulis sangat ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Dosen Pembimbing, Terima kasih karena sudah ACC judul saya tanpa dibaca terlebih dahulu. :D Terimakasih atas kepercayaannya dan telah membimbing saya dalam menyelesaikan buku setebal ini.
2. Orang Tua yang tak kenal lelah menanyakan “Kapan Kamu Lulus Le?”. Terima kasih atas dukungan moril dan materil.
3. Buat Teman-teman 11-S1TI-11, maaf kalian semua tidak saya undang saat ujian skripsi. Ahahaha.. Terimakasih atas senyum yang kalian berikan.
4. Terimakasih buat SitiHamidah tidak bikin aku galau, selama menyelesaikan skripsi ini. titik\_dua\_bintang

Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari kesempurnaan, Karena sempurna hanya milik Allah SWT. Harapan penulis,

informasi dari skripsi ini mampu memberikan manfaat untuk penulis dan pembaca yang masih berjuang dalam perjuangannya.





## 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 Armadyah Amborowati, S.Kom, M. Eng, Ibu Ema Utami, Dr., S.Si., M.Kom dan Bapak Barka Satya, M.Kom. yang telah menguji 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, 15 Desember 2014

Penyusun

## DAFTAR ISI

JUDUL .....	ii
PERSETUJUAN .....	iii
PENGESAHAN .....	iv
PERNYATAAN .....	v
MOTTO .....	vi
PERSEMBAHAN .....	vii
KATA PENGANTAR .....	ix
DAFTAR ISI .....	xi
DAFTAR TABEL .....	xv
DAFTAR GAMBAR .....	xvi
INTISARI .....	xix
<i>ABSTRACT</i> .....	xx
BAB I .....	1
PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	4
1.3 Batasan Masalah .....	4
1.4 Tujuan Penelitian .....	5
1.5 Manfaat Penelitian .....	5
1.6 Metode Penelitian .....	6
1.6.1 Metode Pengumpulan Data .....	6
1.6.2 Metode Analisis Data .....	6

1.6.3	Metode Perancangan Aplikasi .....	7
1.6.4	Metode Implementasi Aplikasi .....	7
1.6.5	Metode Testing .....	7
1.7	Sistematika Penulisan.....	7
<b>BAB II.....</b>		<b>9</b>
<b>LANDASAN TEORI.....</b>		<b>9</b>
2.1	Tinjauan Pustaka .....	9
2.2	Konsep Dasar Informasi.....	10
2.2.1	Pengertian Informasi.....	11
2.2.2	Kualitas Informasi.....	11
2.2.3	Nilai Informasi.....	12
2.3	Konsep Dasar Kriptografi .....	12
2.3.1	Pengertian Kriptografi .....	12
2.3.2	Algoritma Kriptografi .....	15
2.3.3	Tujuan Kriptografi .....	18
2.4	Konsep Dasar Steganografi.....	19
2.4.1	Pengertian Steganografi.....	19
2.4.2	Media Citra Digital .....	20
2.4.3	Least Significant Bit Insertion (LSB) .....	23
2.5	OpenSSL .....	24
2.5.1	Pengertian SSL.....	24
2.5.2	Pengertian OpenSSL.....	25
2.5.3	Fungsi Umum OpenSSL.....	26
2.6	AES .....	27
2.7	MD5 .....	29

2.8	Web .....	32
2.8.1	Pengertian Web .....	32
2.8.2	Pemograman Web .....	33
2.8.3	Komponen Penyusun Web.....	34
2.9	PHP.....	35
2.9.1	Konsep Kerja PHP .....	36
2.9.2	Fungsi PHP .....	37
2.9.3	Oprasi Gambar Pada PHP .....	38
2.10	Teori Analisis SWOT.....	39
2.11	UML .....	40
2.11.1	Usecase Diagram .....	40
2.11.2	Class Diagram.....	43
2.11.3	Sequence Diagram .....	45
2.11.4	Activity Diagram .....	46
BAB III	.....	48
ANALISIS & PERANCANGAN	.....	48
3.1	Gambaran Umum Aplikasi.....	48
3.1.1	Model Sistem Aplikasi Lama .....	49
3.1.2	Model Sistem Aplikasi Baru.....	49
3.2	Analisis SWOT .....	49
3.2.1	Kekuatan ( <i>Strengths</i> ) .....	50
3.2.2	Kelemahan ( <i>Weakness</i> ).....	51
3.2.3	Peluang ( <i>Opportunities</i> ).....	51
3.2.4	Ancaman ( <i>Threats</i> ) .....	52
3.3	Analisis Kebutuhan Sistem .....	53

3.3.1	Analisis Kebutuhan Fungsional.....	53
3.3.2	Analisis Kebutuhan Non Fungsional.....	54
3.4	Analisis Kelayakan Sistem.....	56
3.5	Analisis Data .....	57
3.5.1	Hasil Proses Steganografi LSB.....	57
3.5.2	Hasil Proses OpenSSL dengan AES 128 bit .....	58
3.5.3	Hasil Hitung Manual MD5 .....	60
3.6	Perancangan Sistem.....	61
3.6.1	Perancangan Prosedural.....	61
3.6.2	Perancangan Proses .....	64
3.6.3	Perancangan <i>Interface / Antarmuka</i> .....	76
BAB IV	.....	84
IMPLEMENTASI & PEMBAHASAN	.....	84
4.1	Implementasi .....	84
4.1.1	Implementasi Algoritma .....	85
4.1.2	Implementasi Interface.....	88
4.2	Pembahasan.....	96
4.2.1	Pembahasan Program.....	97
4.2.2	Pengujian Aplikasi.....	99
4.2.4	Hasil Pengujian Aplikasi .....	114
BAB V	.....	120
PENUTUP.....	.....	120
5.1	Kesimpulan.....	120
5.2	Saran.....	121
DAFTAR PUSTAKA .....	.....	123

## DAFTAR TABEL

Tabel 2.1 Estimasi Profile Pengguna Internet di Lima Benua Tahun 2008(Prof.Richardus, 2014).....	10
Tabel 2.2 Hubungan antara jumlah ronde dan panjang kunci AES(Rifki Sadikin, 2012) .....	27
Tabel 2.3 Format Gambar yang didukung GD(Abdul Kadir, 2008).....	39
Tabel 2.4 Simbol-simbol Usecase Diagram(Pribadi Raharja, 2010).....	40
Tabel 2.5 Simbol-simbol Class Diagram (Pribadi Raharja, 2010) .....	43
Tabel 2.6 Simbol-simbol Sequence Diagram(Pribadi Raharja, 2010).....	45
Tabel 2.7 Simbol-simbol Activity Diagram(Pribadi Raharja, 2010).....	46
Tabel 3.8 Spesifikasi Komputer <i>Hardware</i> Web Server .....	54
Tabel 3.9 Spesifikasi <i>Hardware</i> Pengguna <i>Desktop</i> .....	54
Tabel 3.10 Spesifikasi <i>Hardware</i> Pengguna <i>Smartphone</i> .....	55
Tabel 3.11 Spesifikasi Perangkat lunak ( <i>software</i> ).....	55
Tabel 4.12 Hasil ujiacoba enkripsi dengan <i>platform</i> yang berbeda dengan kecepatan 65 Mbps .....	114
Tabel 4.13 Hasil ujicoba enkripsi dengan ukuran file yang berbeda.....	115
Tabel 4.14 Hasil ujicoba deskripsi dengan ukuran file yang berbeda .....	116
Tabel 4.15 Hasil Ujicoba dengan jumlah karakter yang berbeda .....	117
Tabel 4.16 perbedaan ukuran file sebelum dan sesudah enkripsi .....	118

## DAFTAR GAMBAR

Gambar 2.1 Sistem Kriptografi Konvensional (Rifki Sadikin, 2012).....	15
Gambar 2.2 Bagan Proses Penyembunyian dan Pengembalian Data.( Agustinus Noertjahyana dkk,hlm.2) .....	20
Gambar 2.3 gambar bentuk persamaan matriks citra digital (T, Sutoyo et al.2009) .....	21
Gambar 2.4 Contoh Steganografi dengan teknik penyisipan bit pada LSB (Rifki Sadikin,2012) .....	23
Gambar 2.5 Unit data AES(Rifki Sadikin, 2012) .....	28
Gambar 2.6 Proses Umum Enkripsi dan Deskripsi AES(Dony Ariyus, 2008).....	29
Gambar 2.7 Pembuatan algoritma MD5(Rinaldi, 2006).....	31
Gambar 2.8 Skema PHP(Abdul Kadir, 2008).....	37
Gambar 3.9 <i>Use Case Diagram</i> .....	64
Gambar 3.10 <i>Activity Diagram</i> Tentang .....	66
Gambar 3.11 <i>Activity Diagram</i> menghapus file gambar.....	67
Gambar 3.12 <i>Activity Diagram</i> Enkripsi .....	68
Gambar 3.13 <i>Activity Diagram</i> Deskripsi .....	69
Gambar 3.14 <i>Activity Diagram</i> Tentang .....	70
Gambar 3.15 <i>Activity Diagram</i> Rule dan Privacy Police .....	70
Gambar 3.16 <i>Sequence Diagram</i> menu <i>about</i> .....	71
Gambar 3.17 <i>Sequence Diagram</i> Proses Enkripsi .....	72
Gambar 3.18 <i>Sequence Diagram</i> Proses Dekripsi .....	73
Gambar 3.19 <i>Sequence Diagram</i> menu <i>help</i> .....	74
Gambar 3.20 <i>Sequence Diagram</i> Menu <i>Rule</i> dan <i>Privacy police</i> .....	74
Gambar 4.21 <i>Class Diagram</i> .....	75
Gambar 3.22 Tampilan menu utama menggunakan layar <i>desktop</i> .....	76
Gambar 3.23 Tampilan menu utama menggunakan layar <i>smartphone</i> .....	77
Gambar 4.24 Tampilan menu enkripsi menggunakan layar <i>desktop</i> .....	77
Gambar 3.25 Tampilan menu enkripsi menggunakan layar <i>smartphone</i> .....	78
Gambar 3.26 Tampilan menu deskripsi menggunakan layar <i>desktop</i> .....	78



Gambar 3.27 Tampilan menu deskripsi menggunakan layar <i>smartphone</i> .....	79
Gambar 3.28 Tampilan hasil proses enkripsi menggunakan layar <i>desktop</i> .....	79
Gambar 3.29 Tampilan hasil proses enkripsi menggunakan layar <i>smartphone</i> ....	80
Gambar 3.30 Tampilan hasil proses deskripsi menggunakan layar <i>desktop</i> .....	80
Gambar 3.31 Tampilan hasil proses deskripsi menggunakan layar <i>smartphone</i> .....	81
Gambar 3.32 Tampilan menu <i>about</i> .....	81
Gambar 3.33 Tampilan menu <i>help</i> .....	82
Gambar 3.34 Tampilan menu <i>rule and privacy police</i> .....	83
Gambar 4.35 contoh <i>syntax error</i> .....	84
Gambar 4.36 contoh <i>runtime error</i> .....	85
Gambar 4.37 Implementasi tampilan menu utama menggunakan layar <i>desktop</i> ...	89
Gambar 4.38 Implementasi tampilan menu utama menggunakan layar <i>smartphone</i> .....	89
Gambar 4.39 Implementasi tampilan menu enkripsi menggunakan layar <i>desktop</i> 90	90
Gambar 4.40 Implementasi Tampilan menu enkripsi menggunakan layar <i>smartphone</i> .....	90
Gambar 4.41 Implementasi tampilan hasil enkripsi menggunakan layar <i>desktop</i> .91	91
Gambar 4.42 Implementasi tampilan hasil enkripsi menggunakan layar <i>smartphone</i> .....	91
Gambar 4.43 implementasi tampilan menu deskripsi menggunakan layar <i>desktop</i> .....	92
Gambar 4.44 Implementasi tampilan menu deskripsi menggunakan layar <i>smartphone</i> .....	92
Gambar 4.45 Implimentasi ampilan hasil deskripsi menggunakan layar <i>desktop</i> .93	93
Gambar 4.46 Implementasi tampilan hasil deskripsi menggunakan layar <i>smartphone</i> .....	93
Gambar 4.47 Implementasi tampilan menu <i>about</i> .....	94
Gambar 4.48 Implementasi tampilan menu <i>help</i> .....	95
Gambar 4.49 Tampilan menu <i>rule and privacy police</i> .....	96
Gambar 4.50 Installasi xampp .....	100
Gambar 4.51 Installasi Mozila Firefox pada <i>desktop</i> .....	100

Gambar 4.52	Installasi Mozila Firefox pada <i>smartphone</i> .....	101
Gambar 4.53	mengaktifkan Apache pada Xampp .....	101
Gambar 4.54	pengaturan Advanced sharing settings.....	102
Gambar 4.55	pengaturan batasan ukuran file pada <i>apache</i> .....	103
Gambar 4.56	gambar Mozilla firefox bagian address pada <i>desktop</i> .....	103
Gambar 4.57	gambar Mozilla firefox bagian address pada <i>smartphone</i> .....	103
Gambar 4.58	pengujian tampilan menu utama pada layar <i>desktop</i> .....	104
Gambar 4.59	pengujian tampilan menu utama pada layar <i>smartphone</i> .....	104
Gambar 4.60	Pengujian tampilan menu enkripsi pada desktop.....	105
Gambar 4.61	Pengujian tampilan menu enkripsi pada <i>smartphone</i> .....	105
Gambar 4.62	memilih file untuk di proses enkripsi pada <i>desktop</i> .....	106
Gambar 4.63	memilih file untuk di proses enkripsi pada <i>smartphone</i> .....	106
Gambar 4.64	pengujian mengisi form password dan message pada <i>desktop</i> .....	107
Gambar 4.65	pengujian mengisi form password dan message pada <i>smartphone</i> .....	107
Gambar 4.66	pengujian tampilan enkripsi pada <i>desktop</i> .....	108
Gambar 4.67	pengujian tampilan enkripsi pada <i>smartphone</i> .....	108
Gambar 4.68	dialog penyimpanan file terenkripsi.....	109
Gambar 4.69	aktifitas penyimpanan file terenkripsi pada <i>smartphone</i> .....	109
Gambar 4.70	Pengujian tampilan menu deskripsi pada <i>desktop</i> .....	109
Gambar 4.71	Pengujian tampilan menu deskripsi pada <i>smartphone</i> .....	110
Gambar 4.72	memilih file untuk di proses deskripsi pada <i>desktop</i> .....	110
Gambar 4.73	memilih file untuk di proses deskripsi pada <i>smartphone</i> .....	111
Gambar 4.74	pengujian pengisian form password pada <i>desktop</i> .....	111
Gambar 4.75	pengujian pengisian form password pada <i>smartphone</i> .....	112
Gambar 4.76	pengujian tampilan deskripsi pada <i>desktop</i> .....	112
Gambar 4.77	pengujian tampilan deskripsi pada <i>smartphone</i> .....	113
Gambar 4.78	tampilan gambar sebelum dan sesudah enkripsi .....	113
Gambar 4.79	Grafik kecepatan enkripsi dengan file berbeda.....	115
Gambar 4.80	Grafik kecepatan deskripsi dengan ukuran file yang berbeda .....	116
Gambar 4.81	Grafik enkripsi dengan jumlah karakter yang berbeda .....	117
Gambar 4.82	Grafik perbedaan ukuran file sebelum dan sesudah enkripsi.....	118

## INTISARI

Setiap manusia memiliki data ataupun informasi rahasia, dan cara menyimpannya pun setiap orang berbeda-beda. Di jaman modren ini , mereka biasanya menyimpannya pada media komputer atau prangkat elektronik yang dimilikinya. Ada yang di simpan dalam aplikasi catatan atau aplikasi yang mengharuskan penggunaanya untuk login. Aplikasi-aplikasi ini lah yang sering menjadi incaran para pirates untuk diambil data dan informasi rahasianya.

Dengan menggunakan 3 teknik sekaligus dalam mengamankan data dan informasi rahasia diyakini dapat membuat tingkat keamanannya lebih tinggi. Diantaranya dengan Steganografi dimana data dan informasi rahasia tersebut disembunyikan di media digital. OpenSSL yang notabene adalah sebuah perpustakaan kriptografi dan toolkit SSL. Lapisan terkahir adalah Md5 yang berfungsi sebagai pengenkripsi password.

Untuk memudahkan pengguna dalam merahasiakan informasi nya, aplikasi dibuat dalam bentuk web site, dengan begitu pengguna hanya membutuhkan akses internet untuk menyimpan data dan informasi pentingnya ke dalam sebuah media digital. Hasilnya , aplikasi ini bisa berjalan dan bisa melakukan proses enkripsi dan deskripsi pada platform desktop dan smartpone.

**Kata kunci:** OpenSSL, Kriptografi , Steganografi

## **ABSTRACT**

*Everyone has data or confidential information, and how to store them else everyone is different. In this era of modern, they usually save it on computer or electronic media. There are in store in the application note or application that requires users to login. These applications who are often the target of the pirates to take the data and information secret.*

*By using the 3 technique as well as in securing confidential data and information is believed to be able to create a higher security level. Including with Steganography, where data and information the secret hidden in digital media. OpenSSL which incidentally is a library of cryptographic and SSL toolkit. The last layer is the Md5 function as encrypting the password.*

*To facilitate users in their information secret, the application is made in the form of a web site, so users only need access to the internet for storing important data and information into a digital media. As a result, this application can run and can perform the encryption and description process on desktop and smartphone platforms.*

**Keyword:** *OpenSSL, cryptography, Steganography*