

**PENGAMANAN DATA MENGGUNAKAN ALGORITMA  
RANDOM KEY MAES DAN MLSB**

**TUGAS AKHIR**

Oleh:

**HERMAN WIJAYA**

NIM. 15.111.0873

**PUTRA HARDI**

NIM. 15.111.1143

**EDWIN**

NIM. 15.111.0466



**PROGRAM STUDI TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER  
MIKROSKIL  
MEDAN  
2019**

# **DATA SECURITY USING RANDOM KEY MAES AND MLSB ALGORITHM**

## **FINAL PROJECT**

By :

**HERMAN WIJAYA**

NIM. 15.111.0873

**PUTRA HARDI**

NIM. 15.111.1143

**EDWIN**

NIM. 15.111.0466



**STUDY PROGRAM OF INFORMATICS ENGINEERING**

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**

**MIKROSKIL**

**MEDAN**

**2019**

## LEMBARAN PENGESAHAN

### PENGAMANAN DATA MENGGUNAKAN ALGORITMA RANDOM KEY MAES DAN MLSB

#### TUGAS AKHIR

Diajukan untuk melengkapi Persyaratan Guna  
Mendapatkan Gelar Sarjana Strata Satu  
Program Studi Teknik Informatika

Oleh :

HERMAN WIJAYA (NIM. 151110873)  
PUTRA HARDI (NIM. 151111143)  
EDWIN (NIM. 151110466)

Disetujui Oleh :  
Dosen Pembimbing,

Dr. Ronsen Purba, M.Sc.

Medan, 14 Februari 2020

Diketahui dan Disahkan Oleh:



Ketua Program Studi  
Teknik Informatika,  
Gunawan, S.Kom., M.T.I.

## LEMBAR PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Jurusan/Program Studi S-1 Teknik Informatika STMIK Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Herman Wijaya  
Nim : 151110873  
Permintaan : KOMPUTASI ILMIAH

Saya telah melaksanakan penelitian dan penulisan Tugas Akhir dengan judul "PENGAMANAN DATA MENGGUNAKAN ALGORITMA RANDOM KEY MAES DAN MLSB", dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Tugas Akhir tersebut merupakan hasil karya saya sendiri (tidak menyeruuh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun yang dirujuk, telah saya nyatakan dengan benar. Bila dikemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh STMIK Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada STMIK Mikroskil Medan Hak Bebas Royalti Non-ekslusif (Non-exclusive Royalty Free Right) atas Tugas Akhir saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, STMIK Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tugas Akhir saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Tugas Akhir saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 30 Januari 2020

Saya yang membuat pernyataan,



Herman Wijaya

## LEMBAR PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Jurusan/Program Studi S-1 Teknik Informatika STMIK Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Putra Hardi  
Nim : 151111143  
Permintaan : KOMPUTASI ILMIAH

Saya telah melaksanakan penelitian dan penulisan Tugas Akhir dengan judul "PENGAMANAN DATA MENGGUNAKAN ALGORITMA RANDOM KEY MAES DAN MLSB", dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Tugas Akhir tersebut merupakan hasil karya saya sendiri (tidak menyeruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun yang dirujuk, telah saya nyatakan dengan benar. Bila dikemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh STMIK Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada STMIK Mikroskil Medan Hak Bebas Royalti Non-ekslusif (Non-exclusive Royalty Free Right) atas Tugas Akhir saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, STMIK Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tugas Akhir saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Tugas Akhir saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 30 Januari 2020

Saya yang membuat pernyataan,



Putra Hardi

## LEMBAR PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Jurusan/Program Studi S-1 Teknik Informatika STMIK Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Edwin  
Nim : 151110466  
Permintaan : KOMPUTASI ILMIAH

Saya telah melaksanakan penelitian dan penulisan Tugas Akhir dengan judul "PENGAMANAN DATA MENGGUNAKAN ALGORITMA RANDOM KEY MAES DAN MLSB", dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Tugas Akhir tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun yang dirujuk, telah saya nyatakan dengan benar. Bila dikemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh STMIK Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada STMIK Mikroskil Medan Hak Bebas Royalti Non-ekslusif (Non-exclusive Royalty Free Right) atas Tugas Akhir saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, STMIK Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tugas Akhir saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Tugas Akhir saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 30 Januari 2020

Saya yang membuat pernyataan,  
**STMIK MIKROSKIL MEDAN**  
Nomer Tempel : 0096AHF139975504  
6000 Rupiah  
Edwin

## ABSTRAK

Algoritma AES merupakan algoritma kriptografi yang sering digunakan dan sangat efisien di dalam *software* maupun *hardware*. Namun, AES masih memiliki kelemahan terhadap pengacakan kuncinya dan juga memiliki perhitungan yang kompleks pada metode *MixColumns* sehingga membuat waktu enkripsi dan dekripsi menjadi lebih lama. Selain itu untuk meningkatkan keamanan dari data yang dirahasiakan maka digunakan metode steganografi.

Untuk mengatasi masalah – masalah tersebut maka dalam penelitian ini akan digunakan metode *Random Key Advanced Encryption System* (RK-AES) untuk mengatasi masalah pada pengacakan kunci dan metode *Modified Advanced Encryption System* (MAES) untuk mengatasi kompleksitas perhitungan pada *MixColumns*. Untuk metode steganografinya digunakan metode *Modified Least Significant Bit* (MLSB).

Pengujian untuk metode RK-AES dalam pengacakan kunci dibandingkan dengan AES biasanya menghasilkan rata-rata nilai yang cukup baik. Dan pengujian untuk metode MAES dalam segi kecepatan dibandingkan dengan AES biasanya memiliki kecepatan enkrip dan dekrip yang lebih baik. Untuk metode MLSB citra yang disisipkan memiliki nilai MSE dan PSNR yang cukup baik.

Kata kunci: enkripsi, dekripsi, *Random*, AES, MLSB

UNIVERSITAS  
MIKROSKIL

## KATA PENGANTAR

Ucapan syukur kepada Tuhan Yang Maha Esa, atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Tugas Akhir yang berjudul **Aplikasi Pengamanan Data Menggunakan Algoritma Random Key MAES dan MLSB**.

Tugas Akhir ini dibuat untuk melengkapi persyaratan guna memperoleh gelar Sarjana Strata Satu pada Program Studi Teknik Informatika, STMIK Mikroskil Medan. Dalam penyusunan dan penulisan Tugas Akhir ini tidak terlepas dari bantuan, bimbingan serta dukungan dari berbagai pihak. Oleh karena itu pada kesempatan ini, izinkan penulis menyampaikan terima kasih kepada:

1. Bapak Dr. Ronsen Purba, M.Sc., selaku Pembimbing I yang telah membimbing penulis selama mengerjakan Tugas Akhir ini.
2. Ibu Wulan Sri Lestari, S.Kom., selaku Pedamping Pembimbing yang telah membimbing penulis selama mengerjakan Tugas Akhir ini.
3. Bapak Dr. Pahala Sirait, S.T., M.Kom., selaku Ketua STMIK Mikroskil Medan.
4. Bapak Djoni, S.Kom., M.T.I., selaku Wakil Ketua I STMIK Mikroskil Medan.
5. Bapak Gunawan, S.Kom., M.T.I., selaku Ketua Program Studi Teknik Informatika STMIK Mikroskil Medan.
6. Bapak dan Ibu Dosen yang telah mendidik dan membimbing penulis dalam mengerjakan Tugas Akhir ini.
7. Keluarga yang terus memberikan dukungan penuh kepada penulis selama proses penggerjaan Tugas Akhir ini.
8. Semua pihak yang telah membantu penulis dalam proses penulisan tugas akhir ini.

Penulis menyadari bahwa dalam penulisan Tugas Akhir ini masih terdapat kekurangan dan masih jauh dari sempurna. Oleh karena itu, setiap kritik dan saran yang sifatnya membangun akan diterima dengan senang hati. Akhir kata penulis berharap semoga Tugas Akhir ini dapat memberikan manfaat bagi para pembaca.

Medan, 31 Januari 2020

Penulis

## DAFTAR ISI

ABSTRAK .....	i
KATA PENGANTAR .....	ii
DAFTAR ISI.....	iii
DAFTAR GAMBAR .....	vi
DAFTAR TABEL.....	ix
BAB I PENDAHULUAN .....	10
1.1 Latar Belakang .....	10
1.2 Rumusan Masalah .....	11
1.3 Tujuan .....	12
1.4 Manfaat .....	12
1.5 Batasan Masalah .....	12
1.6 Metode Penelitian .....	12
BAB II LANDASAN TEORI .....	14
2.1 Citra Digital .....	14
2.2 Pengenalan Kriptografi .....	16
2.2.1 Definisi .....	17
2.2.2 Terminologi .....	18
2.3 Sistem Kriptografi .....	22
2.3.1 Kriptografi Kunci Simetri .....	22
2.3.2 Kriptografi Kunci Asimetri .....	23
2.4 Landasan Matematika Kriptografi .....	26
2.4.1 Permutasi ( <i>Permutation</i> ) .....	26
2.4.2 Subtitusi .....	26
2.4.3 XOR .....	27
2.4.4 Pergeseran Bit ( <i>Shift</i> ) .....	27
2.4.5 Rotasi Bit ( <i>Rotate</i> ) .....	28
2.5 Algoritma AES ( <i>Advanced Encryption Standard</i> ) .....	29
2.5.1 Notasi .....	29

2.5.2	Konsep Matematika pada Algoritma AES .....	31
2.5.3	Spesifikasi Algortima .....	33
2.5.4	Pembentukan Kunci .....	34
2.5.5	Proses Enkripsi .....	35
2.5.6	Proses Dekripsi .....	38
2.6	Algoritma <i>Modified RK-MAES</i> .....	41
2.7	Steganografi .....	44
2.7.1	Sejarah Steganografi .....	45
2.7.2	Kriteria Steganografi yang Bagus .....	45
2.7.3	Metode Steganografi .....	46
2.7.4	MLSB dengan <i>Random Pixel Selection</i> .....	47
2.8	Penilaian Kualitas Citra .....	51
2.8.1	<i>Mean Square Error</i> .....	51
2.8.2	<i>Peak Signal to Noise Ratio</i> .....	52
	BAB III ANALISIS DAN PERANCANGAN .....	53
3.1	Analisis .....	53
3.1.1	Analisis Proses .....	53
3.1.2	Analisis Kebutuhan .....	145
3.2	Perancangan .....	157
3.2.1	<i>Form</i> Utama .....	157
3.2.2	<i>Form</i> Enkripsi dan Penyisipan .....	158
3.2.3	<i>Form</i> Ekstraksi dan Dekripsi .....	159
3.2.4	<i>Form</i> Pengujian .....	160
3.2.5	<i>Form</i> Pengujian Keamanan Kunci .....	161
3.2.6	<i>Form</i> Pengujian Kecepatan Enkripsi dan Dekripsi .....	162
3.2.7	<i>Form</i> Pengujian Kualitas Citra Stego .....	164
	BAB IV HASIL DAN PENGUJIAN .....	166
4.1	Hasil .....	166
4.1.1	Tampilan Utama .....	166

4.1.2	Tampilan Menu Enkripsi .....	167
4.1.3	Tampilan Menu Dekripsi .....	171
4.1.4	Tampilan Pengujian Program .....	173
4.1.5	Tampilan About .....	177
4.2	Pengujian .....	178
4.2.1	Pengujian Keacakan Kunci dengan Metode RK-AES .....	178
4.2.2	Pengujian Kecepatan Enkripsi dan Dekripsi dengan Metode MAES .....	181
4.2.3	Pengujian Kualitas Citra Stego dari Metode MLSB .....	183
BAB V KESIMPULAN DAN SARAN .....		190
5.1	Kesimpulan .....	190
5.2	Saran .....	190
DAFTAR PUSTAKA .....		191

# UNIVERSITAS MIKROSKIL

## DAFTAR GAMBAR

Gambar 2.1 Citra Diam .....	14
Gambar 2.2 Representasi Citra Digital dalam 2 Dimensi .....	15
Gambar 2.3 <i>Plaintext</i> dan <i>Ciphertext</i> berupa teks .....	18
Gambar 2.4 <i>Plaintext</i> dan <i>Ciphertext</i> berupa gambar .....	19
Gambar 2.5 Enkripsi Data tertentu di dalam Arsip Basisdata .....	20
Gambar 2.6 Skema Enkripsi dan Dekripsi dengan Menggunakan Kunci.....	22
Gambar 2.7 Skema Kriptografi Simetris.....	23
Gambar 2.8 Skema Kriptografi Asimetris .....	24
Gambar 2.9 Sebuah Surat yang Dibubuh Tanda-Tangan Digital .....	25
Gambar 2.10 <i>Input Array of Byte 128 bit</i> .....	30
Gambar 2.11 <i>State Array</i> terdiri atas 4 <i>word</i> .....	30
Gambar 2.12 Transformasi <i>SubBytes()</i> pada State.....	36
Gambar 2.13 Transformasi <i>ShiftRows()</i> pada State .....	36
Gambar 2.14 Transformasi <i>MixColumns()</i> pada State .....	37
Gambar 2.15 Transformasi <i>AddRoundKey()</i> pada State .....	38
Gambar 2.16 Proses Enkripsi dan Dekripsi Menggunakan AES .....	38
Gambar 2.17 Transformasi <i>InvShiftRows()</i> pada <i>State</i> .....	39
Gambar 2.18 Modifikasi Ekspansi Kunci untuk 14 Putaran AES .....	42
Gambar 2.19 Algoritma <i>Modified AES</i> : Tabel <i>Bit Permutation</i> .....	43
Gambar 2.20 Algoritma <i>Modified AES</i> : Tabel <i>Inverse Bit Permutation</i> .....	43
Gambar 2.21 Algoritma Modifikasi AES : Struktur Enkripsi dan Dekripsi .....	44
Gambar 2.22 Segmentasi Citra Berdasarkan Algoritma DSIS .....	48
Gambar 2.23 Algoritma Penyisipan Data pada Citra Sampul.....	50
Gambar 2.24 Algoritma Ekstrasi Data Rahasia .....	51
Gambar 3.1 Proses Enkripsi dan Penyisipan Metode Kriptografi RK-MAES dan Metode Steganografi MLSB .....	53
Gambar 3.2 <i>Flowchart</i> Proses Pembentukan Kunci AES dengan Menggunakan Metode RK-AES .....	55
Gambar 3.3 <i>Flowchart</i> Proses Eksekusi Fungsi SRFG dengan Penambahan RCi	57
Gambar 3.4 <i>Flowchart</i> Proses Kerja Fungsi <i>g</i> .....	61

Gambar 3.5 <i>Flowchart</i> Proses Kerja Fungsi SRFG tanpa Penambahan RCi .....	63
Gambar 3.6 <i>Flowchart</i> Proses Enkripsi Pesan Rahasia dengan Metode MAES ...	98
Gambar 3.7 <i>Flowchart</i> Proses Penyisipan dengan Metode Steganografi MLSB	117
Gambar 3.8 <i>Flowchart</i> Proses Segmentasi Citra dengan Algoritma DSIS.....	118
Gambar 3.9 Pemecahan Citra Sampul .....	119
Gambar 3.10 Hasil Pembagian Segmen dan <i>Gap</i> pada Citra Sampul .....	121
Gambar 3.11 <i>Flowchart</i> Proses Penyisipan <i>Bit Ciphertext</i> .....	122
Gambar 3.12 <i>Flowchart</i> Proses Ekstraksi dan Dekripsi dari Penggabungan Algoritma Kriptografi RK-MAES dan Metode Steganografi MLSB.....	128
Gambar 3.13 <i>Flowchart</i> Proses Ekstraksi Bit dengan Metode Steganografi MLSB .....	129
Gambar 3.14 <i>Flowchart</i> Proses Ekstraksi <i>Bit Ciphertext</i> .....	130
Gambar 3.15 <i>Flowchart</i> Proses Dekripsi <i>Ciphertext</i> dengan Metode MAES .....	136
Gambar 3.16 <i>Use Case Diagram</i> dari Sistem Pengamanan Data .....	146
Gambar 3.17 Rancangan <i>Form</i> Utama.....	158
Gambar 3.18 Rancangan <i>Form</i> Enkripsi dan Penyisipan .....	159
Gambar 3.19 Rancangan <i>Form</i> Ekstraksi dan Dekripsi.....	160
Gambar 3.20 Rancangan <i>Form</i> Pengujian .....	161
Gambar 3.21 Rancangan <i>Form</i> Pengujian Keamanan Kunci .....	162
Gambar 3.22 Rancangan <i>Form</i> Pengujian Kecepatan Enkripsi dan Dekripsi .....	163
Gambar 3.23 Rancangan <i>Form</i> Pengujian Kualitas Citra Stego.....	164
Gambar 4.1 Form Utama.....	166
Gambar 4.2 Form Enkripsi dan Penyisipan .....	167
Gambar 4.3 Tampilan Kotak Dialog <i>Browse</i> .....	167
Gambar 4.4 Tampilan <i>Form</i> Enkripsi dan Penyisipan Setelah Data Tekst Dimasukkan .....	168
Gambar 4.5 Tampilan <i>Form</i> Enkripsi dan Penyisipan Setelah Data Tekst dan Kunci Rahasia Diproses menjadi <i>Ciphertext</i> .....	168
Gambar 4.6 Tampilan Dialog Kotak “...” .....	169
Gambar 4.7 Tampilan <i>Form</i> Enkripsi dan Penyisipan Setelah Memasukkan Citra Sampul .....	169
Gambar 4.8 Tampilan <i>Form</i> Enkripsi dan Penyisipan Setelah Semua Data	

Dimasukkan dan <i>User</i> Mengklik Tombol “Proses Penyisipan” .....	170
Gambar 4.9 Kotak Dialog “Simpan Citra Stego” .....	170
Gambar 4.10 Tampilan Menu Dekripsi .....	171
Gambar 4.11 Tampilan Dialog Kotak “...” .....	171
Gambar 4.12 Tampilan Setelah <i>User</i> Memasukkan Gambar.....	172
Gambar 4.13 Tampilan Setelah User Memasukkan Gambar dan Kunci Ks.....	172
Gambar 4.14 Tampilan <i>Form</i> Setelah Proses Ekstraksi dan Dekripsi .....	173
Gambar 4.15 Tampilan <i>Form</i> Pengujian.....	173
Gambar 4.16 Tampilan <i>Form</i> Kemanan Kunci.....	174
Gambar 4.17 Tampilan <i>Form</i> Keamanan Kunci Setelah Kunci Diproses .....	174
Gambar 4.18 Tampilan <i>Form</i> Pengujian Kecepatan Enkripsi dan Dekripsi MAES .....	175
Gambar 4.19 Tampilan <i>Form</i> Pengujian Kecepatan Enkripsi dan Dekripsi MAES Setelah Diproses.....	176
Gambar 4.20 Tampilan <i>Form</i> Pengujian Kualitas Citra Stego dari Metode MLSB .....	176
Gambar 4.21 Tampilan <i>Form</i> Pengujian Kualitas Citra Stego dari Metode MLSB Setelah Memproses Citra .....	177
Gambar 4.22 Tampilan <i>Form About</i> .....	178
Gambar 4.23 Kumpulan Citra dengan berbagai ukuran dan kepadatan warna....	183

# UNIVERSITAS MIKROSKIL

## DAFTAR TABEL

Tabel 2.1 Kode Warna .....	16
Tabel 2.2 Operasi XOR untuk bit .....	27
Tabel 2.3 Hubungan antara ukuran kunci, ukuran blok dengan jumlah putaran .....	33
Tabel 2.4 Rcon dengan i dimulai dari 1 sampai 10 dalam bentuk heksadesimal.....	34
Tabel 2.5 Tabel S-box .....	35
Tabel 2.6 Tabel <i>Inverse S-box</i> .....	39
Tabel 3.1 <i>Use Case Input</i> Citra .....	146
Tabel 3.2 <i>Use Case Input</i> Pesan.....	148
Tabel 3.3 <i>Use Case Input</i> Kunci .....	148
Tabel 3.4 <i>Use Case</i> Melakukan Proses Enkripsi dan Penyisipan .....	150
Tabel 3.5 <i>Use Case</i> Melakukan Proses Ekstraksi dan Dekripsi .....	151
Tabel 3.6 <i>Use Case</i> Melakukan Proses Pengujian Keamanan Kunci .....	152
Tabel 3.7 <i>Use Case</i> Melakukan Proses Pengujian Kecepatan Enkripsi dan Dekripsi .....	154
Tabel 3.8 <i>Use Case</i> Melakukan Proses Pengujian Kualitas Citra Stego .....	150
Tabel 4.1 Tabel Hasil Pengujian Keacakan Kunci dengan Metode RK-AES .....	179
Tabel 4.2 Tabel Hasil Pengujian Kecepatan Enkripsi dan Dekripsi .....	182
Tabel 4.3 Tabel Data Pengujian pada Citra (a) .....	184
Tabel 4.4 Tabel Data Pengujian pada Citra (b).....	184
Tabel 4.5 Tabel Data Pengujian pada Citra (c) .....	185
Tabel 4.6 Tabel Data Pengujian pada Citra (d).....	186
Tabel 4.7 Tabel Data Pengujian pada Citra (e).....	186
Tabel 4.8 Tabel Hasil Pengujian Kualitas Citra pada Citra (a).....	187
Tabel 4.9 Tabel Hasil Pengujian Kualitas Citra pada Citra (b).....	188
Tabel 4.10 Tabel Hasil Pengujian Kualitas Citra pada Citra (c).....	188
Tabel 4.11 Tabel Hasil Pengujian Kualitas Citra pada Citra (d).....	188
Tabel 4.12 Tabel Hasil Pengujian Kualitas Citra pada Citra (e).....	189