

**KOMPARASI KRIPTOGRAFI AES DAN RC4 PADA
METODE LEAST SIGNIFICANT BIT (LSB) PADA CITRA
DIGITAL DENGAN FORMAT BITMAP**

TESIS



PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2017

**KOMPARASI KRIPTOGRAFI AES DAN RC4 PADA
METODE LEAST SIGNIFICANT BIT (LSB) PADA CITRA
DIGITAL DENGAN FORMAT BITMAP**

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)



Oleh:

Rahmat Sulaiman

1511601740

PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2017



PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Nama Mahasiswa : RAHMAT SULAIMAN
Nomor Induk Mahasiswa : 1511601740
Konsentrasi : Rekayasa Komputasi Terapan
Fakultas / Program : Magister Ilmu Komputer
Jenjang Studi : Strata 2

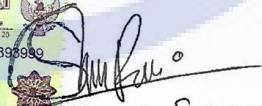
Mennytakan bahwa TESIS yang berjudul :

KOMPARASI KRİPTOGRAFI AES DAN RC4 PADA METODE
LEAST SIGNIFICANT BIT (LSB) PADA CITRA DIGITAL
DENGAN FORMAT BITMAP

1. Merupakan hasil karya tulis ilmiah sendiri bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. Saya izinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku,

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila dikemudian hari pernyataan ini tidak benar.

Tebarta, 8 Agustus 2017


Rahmat Sulaiman,





PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Rahmat Sulaiman
Nomor Induk Mahasiswa : 1511601740
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Judul Tesis : KOMPARASI KRIPTOGRAFI AES DAN RC4
PADA METODE LEAST SIGNIFICANT BIT (LSB)
PADA CITRA DIGITAL DENGAN FORMAT
BITMAP

Jakarta, 4 Agustus 2017

Tim Penguji
Ketua,

Tanda Tangan

(Prof. Dr. Moedjiono, M.Sc)
Anggota,

(Deni Mahdiana, M.M, M.Kom)
Pembimbing Utama

(Dr. Ir. Nazori AZ, M.T)

Ketua Program Studi
Magister Ilmu Komputer

(Dr. M. Syafrullah, M.Kom, M.Sc)

ABSTRAK

Keamanan pesan merupakan suatu hal yang harus dijaga kerahasiaannya. Namun, untuk menjaga keamanan dan kerahasiaan suatu pesan dibutuhkan dua buah metode yang berbeda. Untuk menjaga keamanan pesan, ilmu yang telah banyak digunakan adalah dengan menggunakan kriptografi. Sedangkan untuk menjaga kerahasiaan pesan, ilmu yang digunakan adalah steganografi. Untuk itu dibutuhkan suatu pengamanan pesan yang dapat menjaga keamanan dan kerahasiaan pesan secara bersamaan. Berbagai algoritma telah banyak diterapkan dalam pengamanan data, namun tidak diketahui algoritma mana yang memiliki kecepatan yang lebih unggul jika diterapkan dalam LSB. Pengujian dilakukan dengan menghitung lama proses waktu enkripsi dan dekripsi dari masing-masing algoritma dengan jumlah pesan dan panjang kunci yang sama. Pengukuran waktu dilakukan sebanyak 10 kali, kemudian diambil nilai rata-ratanya untuk mendapatkan waktu yang konsisten karna ketidakstabilan sistem. Oleh karena itu, akan dilakukan perbandingan kecepatan proses enkripsi dan dekripsi dengan menerapkan algoritma AES dan RC4 pada LSB menggunakan Microsoft Visual Studio 2008. Hasil penelitian proses enkripsi dan dekripsi yang dilakukan, algoritma AES lebih unggul dalam hal kecepatan dibandingkan dengan algoritma RC4. Nilai MSE dan PSNR yang dihasilkan dari gambar yang sudah dienkripsi berdasarkan algoritma AES dan RC4 tidak mengalami perbedaan nilai yang signifikan. Pada penelitian ini secara keseluruhan membuktikan bahwa algoritma AES lebih baik dalam hal kecepatan jika diterapkan pada LSB dibandingkan dengan algoritma RC4.

Kata Kunci: Kriptografi, Steganografi, LSB, AES, RC4

ABSTRACT

Message security is something that must be kept secretly. However, to maintain the security and the secret of a message it takes two different methods. To maintain the security of messages, the science that has been widely used is to use cryptography. As for maintaining the secret of the message, the science used is steganography. For that we need a security message that can maintain the security and the secret of the message simultaneously. Various algorithms have been widely applied in data security, but it is unknown which algorithm has a superior speed when applied in the LSB. The test is done by calculating the length of the encryption time process and the decryption time process of each algorithm with the same number of messages and key lengths. Measurement time is done as much as 10 times, then taken average value to get consistent time because system instability. Therefore, we will compare the speed of encryption and decryption process by applying AES and RC4 algorithm to LSB in Visual Studio 2008. In the process of encryption and decryption, the AES algorithm is superior in terms of speed compared to RC4 algorithm. The MSE and PSNR values generated from the encrypted images based on the AES and RC4 algorithm doesn't show significant value. Overall the AES algorithm is better than RC4 algorithm when applied in LSB.

Keywords: Cryptography, Steganography, LSB, AES, RC4

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah SWT, Tuhan Yang Maha Esa, karena berkat nikmat dan rahmat-Nya penulis bisa menyelesaikan laporan penelitian tesis ini. Tujuan dari penulisan laporan penelitian tesis ini adalah sebagai salah satu syarat untuk menyusun tesis pada Program Studi Magister Ilmu Komputer, Universitas Budi Luhur Jakarta.

Rasa dan ucapan serta ungkapan terima kasih penulis persembahkan kepada semua pihak yang telah membantu penulis dalam menyusun laporan penelitian tesis ini baik secara materiil dan moril:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Ibu saya yang tercinta, yang tidak pernah berhenti memberikan dukungan kepada penulis, baik dalam bentuk moril, materiil, do'a serta kasih sayang yang luar biasa.
3. Kakak-kakak saya yang tercinta yang selalu mendukung dan memberikan semangat yang tiada henti-hentinya kepada penulis.
4. Bapak Drs. Djaetun HS yang telah mendirikan Universitas Budi Luhur.
5. Bapak Drs. Harry Sudjikianto, MM, MBA selaku ketua pengurus harian yayasan Atma Luhur yang telah memberikan Beasiswa kepada penulis.
6. Bapak Dr. Ir. Nazori AZ, M.T, selaku dosen pembimbing tesis yang telah membimbing dan memotivasi penulis dalam mengerjakan penelitian tesis ini.
7. Bpak Dr. Suhartono, M.A, MBA selaku Direktur Program Pasca Sarjana dan Bapak Dr. M. Syafrullah, M.Kom., M.Sc selaku Kaprodi MKom beserta Bapak dan Ibu Dosen pengampu mata kuliah di Program Studi Magister Ilmu Komputer Universitas Budi Luhur yang telah dengan sabar dan tulus memberikan ilmu pengetahuan, pencerahan, dan bimbingan dalam belajar.
8. Rekan-rekan mahasiswa MKOM Universitas Budi Luhur, terima kasih atas kebersamaan, kerja keras dan dukungan semangatnya.
9. Thanks to my best roommate, Tri Sugihartono.

Penulis menyadari masih banyak kekurangan dari laporan penelitian tesis ini, oleh karena itu penulis mengharapkan kritik dan saran yang bersifat membangun demi kesempurnaan penelitian tesis ini. Semoga penelitian tesis ini masih dapat memberikan manfaat dari keterbatasannya. *Amin*.

Jakarta, Agustus 2017

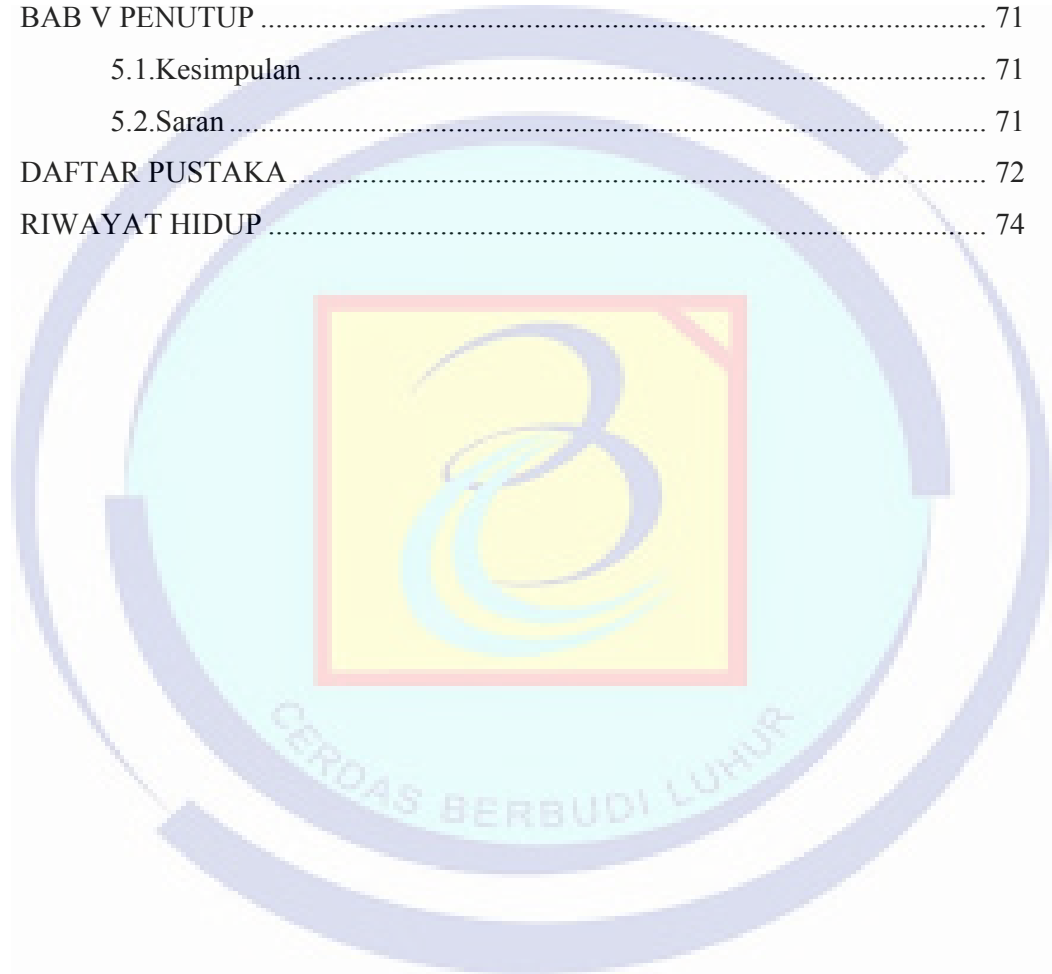
Rahmat Sulaiman

DAFTAR ISI

	Halaman
ABSTRAK	i
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL	ix
 BAB I PENDAHULUAN.....	 1
1.1.Latar Belakang	1
1.2.Masalah Penelitian	2
1.2.1. Identifikasi Masalah	2
1.2.2. Batasan Masalah	3
1.2.3. Rumusan Masalah	3
1.3.Tujuan dan Manfaat.....	3
1.3.1. Tujuan Penelitian	3
1.3.2. Manfaat Penelitian	3
1.4.Tata Urut Penulisan	4
1.5.Daftar Pengertian.....	5
 BAB II LANDASAN TEORI DAN KERANGKA KONSEP	 6
2.1.Landasan Teori.....	6
2.2.Kriptografi.....	6
2.2.1 <i>Advanced Encryption Standard (AES)</i>	9
2.2.2 <i>Rivest Code 4 (RC4)</i>	15
2.3.Steganografi	20
2.3.1 <i>Least Significant Bit (LSB)</i>	24
2.4. <i>Mean Square Error (MSE)</i> dan <i>Peak Signal to Noise Ratio (PSNR)</i> ..	25
2.5.Microsoft Visual Studio 2008	27
2.6.MATLAB (<i>Matrix Laboratory</i>)	28

2.7. Tinjauan Studi	29
2.8. Tinjauan Obyek Penelitian.....	38
2.9. Kerangka Konsep	39
2.10. Hipotesis.....	40
 BAB III METODOLOGI DAN RANCANGAN	41
3.1. Metode Penelitian.....	42
3.2. Instrumentasi	42
3.2.1 Perangkat Keras	42
3.2.2 Perangkat Lunak.....	42
3.3. Teknik Analisis	43
3.4. Langkah-langkah Penelitian.....	43
3.4.1. Pemilihan Obyek Penelitian	43
3.4.2. Perumusan Masalah	44
3.4.3. Studi Pustaka dan Tinjauan Studi	44
3.4.4. Formulasi Hipotesis	44
3.4.5. Desain Pengembangan Sistem.....	44
3.4.5.1 Desain Sistem Kriptografi	45
3.4.5.2 Desain Sistem Steganografi.....	46
3.4.5.3 Desain Sistem Kombinasi.....	48
3.5. Analisis dan Pengujian	51
3.6. Kesimpulan	51
3.7. Jadwal Penelitian.....	52
 BAB IV PEMBAHASAN DAN HASIL PENELITIAN	54
4.1. Analisa Algoritma Kriptografi.....	54
4.2. Hasil Implementasi.....	54
4.3. Pengujian dan Hasil Pengujian.....	57
4.3.1. Pengujian Sistem	57
4.3.2. Hasil Pengujian.....	66
4.4. Implikasi Penelitian	68

4.4.1.Aspek Sistem.....	68
4.4.2.Aspek Manajerial	68
4.4.3.Aspek Penelitian Lanjutan	68
4.5.Rencana Implementasi Sistem	69
 BAB V PENUTUP	 71
5.1.Kesimpulan	71
5.2.Saran	71
DAFTAR PUSTAKA	72
RIWAYAT HIDUP	74



DAFTAR GAMBAR

Gambar	Halaman
II-1. Skema Enkripsi dan Dekripsi Menggunakan Kunci.....	8
II-2. Ilustrasi transformasi <i>SubByte</i>	12
II-3. Ilustrasi transformasi <i>ShiftRows</i>	12
II-4. Ilustrasi transformasi <i>MixColumn</i>	13
II-5. Ilustrasi transformasi <i>AddRoundKey</i>	13
II-6. Alur proses enkripsi algoritma AES, key 128-bit.....	14
II-7. Alur proses dekripsi algoritma AES, key 128-bit.....	15
II-8. Diagram Proses Enkripsi.....	17
II-9. Icon BITMAP	21
II-10. Icon JPEG	22
II-11. Icon GIF.....	22
II-12. MSB dan LSB	25
II-13. Kerangka Konsep	40
III-1. Tahapan Penelitian	44
III-2. Proses Enkripsi.....	46
III-3. Flowchart Proses Enkripsi	46
III-4. Proses Dekripsi	47
III-5. Flowchart Proses Dekripsi	47
III-6. Proses Penyisipan Bit Pada Gambar	48
III-7. Flowchart Proses Penyisipan Bit Pada Gambar.....	48
III-8. Proses Pengembalian Bit ke Plaintext.....	49
III-9. Flowchart Proses Pengembalian Bit ke Plaintext.....	49
III-10. Proses Enkripsi Kombinasi.....	50
III-11. Flowchart Proses Enkripsi Kombinasi.....	50
III-12. Proses Ekstraksi Kombinasi.....	51
III-13. Flowchart Proses Ekstraksi Kombinasi	52
IV-1. Menu Utama.....	54
IV-2. Menu RC4.....	54
IV-3. Menu AES.....	56

IV-4. Menu MSE dan PSNR.....	56
IV-5. Enkripsi RC4 100 Karakter.....	58
IV-6. Enkripsi AES 100 Karakter	58
IV-7. Dekripsi RC4 100 Karakter	59
IV-8. Dekripsi AES 100 Karakter	59
IV-9. Enkripsi RC4 1000 Karakter.....	60
IV-10. Enkripsi AES 1000 Karakter	61
IV-11. Dekripsi RC4 1000 Karakter	61
IV-12. Dekripsi AES 1000 Karakter.....	62
IV-13. MSE dan PSNR RC4 dengan 100 karakter	62
IV-14. MSE dan PSNR AES dengan 100 karakter.....	62
IV-15. MSE dan PSNR RC4 dengan 1000 karakter.....	63
IV-16. MSE dan PSNR AES dengan 1000 karakter.....	63
IV-17. Grafik Batang Pengujian Enkripsi RC4 dan AES	64
IV-18. Grafik Garis Pengujian Enkripsi RC4 dan AES	64
IV-19. Grafik Batang Pengujian Dekripsi RC4 dan AES	66
IV-20. Grafik Garis Pengujian Dekripsi RC4 dan AES.....	66
IV-21. Grafik Pengujian nilai MSE RC4 dan AES.....	67
IV-22. Grafik Pengujian nilai PSNR RC4 dan AES.....	68

DAFTAR TABEL

Tabel	Halaman
II-1. Perbandingan Panjang Kunci AES	11
II-2. S-Box Algoritma AES	12
II-3. Invers S-Box Algoritma AES	13
II-4. Perbandingan Tinjauan Studi	33
III-1. Jadwal Penelitian	53
IV-1. Pengujian enkripsi dengan 100 karakter	57
IV-2. Pengujian dekripsi dengan 100 karakter	58
IV-3. Pengujian enkripsi dengan 1000 karakter	60
IV-4. Pengujian dekripsi dengan 1000 karakter	61
IV-5. Pengujian Waktu Enkripsi	64
IV-6. Pengujian Waktu Dekripsi	65
IV-7. Pengujian Nilai MSE	67
IV-8. Pengujian Nilai PSNR	68
IV-9. Rencana Implementasi Sistem	70

DAFTAR PUSTAKA

- Bruice, S. 2007, *Applied Cryptography, Cryptography Protocols, Algorithm and Source Code in C*, Second edition. Wiley India edition
- Katzenbeisser, FAP. 2000, *Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, Norwood.
- Simmons, G.J. 2000, *The prisoners' problem and the subliminal channel in Proc. Advances in Cryptology*
- Cheddad, A., Joan, C., Curran, K. & Paul, M.K. 2010, *Digital image steganography: Survey and analysis of current methods Signal Processing* 90
- Rian, A. & Lucky, T.O. 2013, *Artikel Implementasi Kriptografi dan Steganografi Menggunakan Algoritma RSA dan Metode LSB*
- N.P, Indah, F.A. & Awang, H.K. 2015, *Jurnal Implementasi Kriptografi Pengamanan Data Pada File Teks, Isi File Dokumen dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard*. Jurnal Informatika Mulawarman Vol. 10 No.1
- Putri, A. 2009, *Artikel Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital*, Mahasiswa Jurusan Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Gunadarma
- Adetya, K.P. *Pengamanan Data Dengan Metode Advanced Cryption Standard dan Metode Least Significant Bit*, Mahasiswa Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang.
- Gede, W.B, & Made, I.W. 2015, *Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB pada Gambar Bitmap*, Jurnal Ilmiah Ilmu Komputer, Universitas Udayana, Vol. 8, No. 2, September
- Handa, G., *Penggunaan Metode Steganografi dan Kriptografi Dengan Algoritma RC4 Stream Cipher Dalam Penganan Citra Digital Perusahaan*, Mahasiswa Pasca Sarjanan, Universitas Budi Luhur
- Hartono, B. 2004, *Ruang Lingkup Kriptografi Untuk Mengamankan Data*, Jurnal Dinamika Informatika, Vol.9, No.2 1-8
- Dony, A. 2005, *Computer Security*, Yogyakarta, Penerbit Andi Yogyakarta, 2005
- Nurhayati & Syukuri, S.H. 2014, *Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm*, Informatics Engineering Department, Science and Technology Faculty Syarif Hidayatullah State Islamic University (UIN) Jakarta,.