



**ANALISIS PENERAPAN KRIPTOGRAFI SEBAGAI SOLUSI KEAMANAN
INFORMASI PADA SISTEM INFORMASI PERENCANAAN DAN
AKUNTABILITAS KINERJA LEMBAGA SANDI NEGARA**

TESIS

Oleh :

RANGGA ADITYA SUTOPO, S.ST

NPM : 111.0921.053

**PROGRAM PASCA SARJANA
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”
JAKARTA
2014**



**ANALISIS PENERAPAN KRIPTOGRAFI SEBAGAI SOLUSI KEAMANAN
INFORMASI PADA SISTEM INFORMASI PERENCANAAN DAN
AKUNTABILITAS KINERJA LEMBAGA SANDI NEGARA**

TESIS

**Diajukan Untuk memenuhi Persyaratan Dalam Memperoleh Gelar
Magister Manajemen
Konsentrasi Manajemen Sistem Informasi**

Oleh :

RANGGA ADITYA SUTOPO, S.ST

NPM : 111.0921.053

**PROGRAM PASCA SARJANA
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”
JAKARTA
2014**

TESIS

**ANALISIS PENERAPAN KRIPTOGRAFI SEBAGAI SOLUSI KEAMANAN
INFORMASI PADA SISTEM INFORMASI PERENCANAAN DAN
AKUNTABILITAS KINERJA LEMBAGA SANDI NEGARA**

Disiapkan dan disusun oleh :

RANGGA ADITYA SUTOPO, S.ST

NPM : 111.0921.053

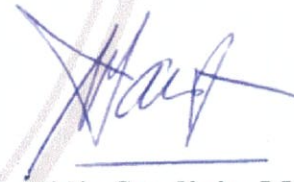
Telah dipertahankan di depan Tim Penguji
Pada Tanggal: 7 Maret 2014
maka dinyatakan telah memenuhi syarat untuk diterima

Pembimbing I



Prof. Dr. Ir. Jafar Basri, M.Sc

Pembimbing II



Dr. Nidjo Sandjojo, M.Sc

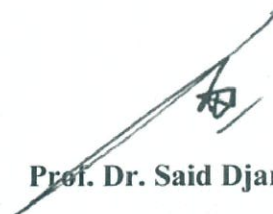
Universitas Pembangunan Nasional "Veteran" Jakarta
Program Pascasarjana

Direktur



Dr. H. M. Aris Munandar, MPA

Ka. Progdi



Prof. Dr. Said Djamaluddin

MOTTO

*Mulailah
Karena dengan memulai, setengah pekerjaan telah selesai*

*Penulis Persembahkan Tesis ini kepada
Mamah, Papah dan Istriku Tercinta*

KATA PENGANTAR

Puji dan syukur selalu terpanjatkan ke hadirat Allah SWT Sang Penguasa Alam Raya yang atas Rahmat dan Karunia-Nya penulis dapat menyelesaikan Tesis yang berjudul “**Analisis Penerapan Kriptografi Sebagai Solusi Keamanan Informasi Pada Sistem Informasi Perencanaan dan Akuntabilitas Kinerja Lembaga Sandi Negara**” ini. Sebagai syarat kelulusan dalam menyelesaikan pendidikan pasca sarjana di Universitas Pembangunan Nasional “Veteran” Jakarta. Shalawat dan salam selalu tercurah kepada Pemimpin Agung, Nabi Besar Muhammad SAW yang telah membawa kita pada zaman terang benderang yang penuh dengan ilmu pengetahuan.

Penulis menyadari bahwa penyusunan Tesis ini bukanlah semata-mata hasil kerja penulis seorang diri, terdapat bantuan dan bimbingan baik moril maupun materiil yang terus mengalir dari berbagai pihak, sehingga Tesis ini terselesaikan dengan baik. Oleh karena itu, pada kesempatan ini dengan penuh rasa hormat penulis bermaksud mengucapkan terima kasih dan penghargaan sebesar-besarnya kepada :

1. Dr. Koesnadi Kardi, M.Sc., RCDS, selaku Rektor Universitas Pembangunan Nasional “Veteran” Jakarta.
2. Dr. H. M. Aris Munandar, MPA. selaku Direktur Program Pascasarjana Universitas Pembangunan Nasional "Veteran" Jakarta.
3. Prof. Dr. Said Djamaluddin, Ph.D. selaku Ketua Program Magister Manajemen Universitas Pembangunan Nasional "Veteran" Jakarta.
4. Prof. Dr. Ir. Jafar Basri, M.Sc. selaku Dosen Pembimbing Utama yang selalu memberi arahan dan masukan dalam penulisan proposal tesis ini.
5. Dr. Nidjo Sandjojo, M.Sc, selaku Pembimbing Pendamping yang telah memberikan saran dan masukan dalam penulisan proposal tesis ini.
6. Dosen Pengajar Program Pascasarjana Universitas Pembangunan Nasional "Veteran" Jakarta.

7. Seluruh Staf Manajemen Program Pascasarjana Universitas Pembangunan Nasional "Veteran" Jakarta.
8. Istri tercintaku Paramitha dan Calon anakku yang selalu mendukung lahir batin, dunia dan akhirat;
9. Papah, Mamah, Abak, Mamak, Citra, Dimas, Mas Jay, Abi, Dhea dan Pooja atas doa yang tak terputus untuk kebaikan dan kebahagiaan anak-anak dan saudaranya.
10. Pimpinan beserta rekan-rekan di Lembaga Sandi Negara atas dukungannya kepada penulis.
11. Rekan-rekan PPS Angkatan 66 dan 63 Universitas Pembangunan Nasional "Veteran" Jakarta yang sedang berjuang bersama-sama dalam menyelesaikan penelitian;
12. Pihak-pihak yang tidak dapat disebutkan namanya satu persatu.

Semoga keikhlasan pihak-pihak yang membantu akan membawa kepada Ridho Allah SWT dan amal ibadahnya diterima di sisi-Nya. Sebagai manusia tempat salah dan lupa, penulis menyadari masih terdapat banyak kekurangan dalam penyusunan Tesis ini. Oleh karena itu, kritik dan saran yang membangun penulis harapkan untuk menyempurnakan tulisan-tulisan selanjutnya. Semoga penulisan Tesis ini dapat bermanfaat bagi siapa saja yang membacanya, khususnya civitas akademika Universitas Pembangunan Nasional "Veteran" Jakarta.

Jakarta, Maret 2014

RAS

DAFTAR ISI

HALAMAN PENGESAHAN	i
MOTTO	ii
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	v
DAFTAR TABEL	vi
DAFTAR LAMPIRAN	vii
RIWAYAT HIDUP PENELITI	viii
PERNYATAAN ORISINALITAS	ix
ABSTRACT	x
BAB I PENYAJIAN MASALAH PENELITIAN	1
1.1. Latar Belakang Masalah.....	1
1.2. Identifikasi Masalah	3
1.3. Ruang Lingkup Penelitian.....	4
1.4. Perumusan Masalah	4
1.5. Tujuan Dan Kegunaan Penelitian.....	5
BAB II KAJIAN PUSTAKA DAN KERANGKA PEMIKIRAN	6
2.1. Hasil Penelitian yang Relevan	6
2.2. Teori yang Mendukung	8
2.3. Kerangka Pemikiran Penelitian.....	29
2.4. Rumusan Hipotesis	30
BAB III METODOLOGI PENELITIAN	31
3.1. Posisi Studi.....	31
3.2. Metoda Penelitian.....	31
3.3. Teknik Pengumpulan Data.....	31
3.4. Subyek Penelitian.....	33
3.5. Teknik Pengolahan dan Pemeriksaan Keabsahan Data	34
3.6. Teknik Analisis Data.....	36

BAB IV ANALISIS DATA	49
4.1. Tahapan Inisisasi.....	49
a. Pengumpulan Dokumen Arsitektur Organisasi dan Keterlibatan Mitra Bisnis	49
b. Identifikasi Peraturan dan Kebijakan yang Terkait.....	63
c. Membangun Tujuan Keamanan	66
d. Kategorisasi Keamanan Informasi dan Sistem Informasi Organisasi.....	70
e. Identifikasi Metode Kriptografi	73
f. Persiapan melakukan <i>Risk Assessment</i>	75
4.2. Tahap Pengembangan	79
a. <i>Risk Assessment</i>	79
b. Pemilihan <i>Initial Baseline of Security Control</i>	82
c. Penentuan metode kriptografi	91
BAB V SIMPULAN DAN SARAN	107
5.1. Simpulan	107
5.2. Saran.....	108
DAFTAR PUSTAKA	110
LAMPIRAN-LAMPIRAN	114

DAFTAR GAMBAR

	Halaman
Gambar 2.1. Transformasi menuju <i>e-government</i>	19
Gambar 2.2. Kerangka arsitektur <i>e-government</i>	20
Gambar 2.3. Kerangka Pemikiran	29
Gambar 3.1. SDLC.....	36
Gambar 3.2. <i>Risk Assessment</i>	41
Gambar 4.1. Pilar Sistem Pembangunan Nasional.....	49
Gambar 4.2. Konsepsi Dasar KPJM dalam RKAKL	53
Gambar 4.3. Persentase kerawanan dan ancaman untuk aspek kerahasiaan....	79
Gambar 4.4. Persentase kerawanan dan ancaman untuk aspek integritas.....	80
Gambar 4.5. Persentase kerawanan dan ancaman untuk aspek ketersediaan...	81

DAFTAR TABEL

	Halaman
Tabel 2.1. Parameter Algoritma AES.....	13
Tabel 2.2. Varian SHA	16
Tabel 3.1. Daftar Informan Pokok.....	33
Tabel 3.2. Daftar Informan Kunci	34
Tabel 3.3. Nilai <i>Likelihood</i>	16
Tabel 3.4. Nilai Dampak	33
Tabel 3.5. Penentuan Tingkat Resiko.....	34
Tabel 4.1. Klasifikasi Aset	66
Tabel 4.2. Jenis dan Klasifikasi Aset SIPAK.....	67
Tabel 4.3. Sasaran Keamanan SIPAK Lemsaneg	68
Tabel 4.4. Sasaran Keamanan dan Dampak Potensial Berdasarkan FIPS 199	70
Tabel 4.5. Identifikasi Ancaman dan Kerawanan	76
Tabel 4.6. Klasifikasi dan Definisi <i>Likelihood</i>	77
Tabel 4.7. Penentuan Dampak.....	78
Tabel 4.8. <i>Security Control</i> dari NIST SP 800-53	82
Tabel 4.9. <i>Initial Baseline of Security Control</i>	84
Tabel 4.10. Risiko dan Solusi Menangani Risiko Menggunakan Kriptografi	92
Tabel 4.11. Daftar Spesifikasi <i>Cipher</i> dalam <i>E-Government</i>	93
Tabel 4.12. Algoritma Standar yang Disetujui NIST (Amerika Serikat).....	95
Tabel 4.13. Standar Algoritma yang Disetujui oleh BSI-Jerman : 2011.....	95
Tabel 4.14. Standar Algoritma yang Disetujui FNISA - Perancis : 2010	96
Tabel 4.15. Perbandingan Performa Algoritma AES dan 3DES.....	97
Tabel 4.16. Persyaratan Panjang Kunci Minimal untuk Keamanan Informasi Rahasia dan Sangat Rahasia	99
Tabel 4.17. Standar Algoritma Hash Berdasarkan NIST	100
Tabel 4.18. Kriptografi pada SSL/TLS	103
Tabel 4.19. Rekomendasi <i>Client Cipher Suites</i>	104
Tabel 4.20. Rekomendasi <i>Server Cipher Suites</i>	105

DAFTAR LAMPIRAN

	Halaman
LAMPIRAN 1	114
LAMPIRAN 2	124



RIWAYAT HIDUP

Penulis dilahirkan di Bogor pada tanggal 3 Februari 1989 dari ayah Sutopo dan Ibu Maharani Dewi. Penulis merupakan putra pertama dari tiga bersaudara dan pada tanggal 7 Desember 2013 telah menikah dengan Paramitha. Penulis lulus Sekolah Tinggi Sandi Negara pada tahun 2010 dan meneruskan program pasca sarjana di Universitas Pembangunan NASional “Veteran” Jakarta pada program studi Magister Manajemen pada tahun 2011.

Riwayat pekerjaan sampai dengan saat ini telah menjadi pegawai negeri sipil di Lembaga Sandi Negara.

Jakarta, Maret 2014
Mahasiswa

Rangga Aditya Sutopo, S.ST
NPM. 111.0921.053

PERNYATAAN ORISINALITAS TESIS

Saya menyatakan dengan sebenar-benarnya bahwa di dalam naskah tesis ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata dalam naskah tesis ini dapat dibuktikan terdapat unsur –unsur jiplakan, saya bersedia Tesis dibatalkan, serta diproses sesuai peraturan perundang-undangan yang berlaku (UU. No. 20 tahun 2003, pasal 25 ayat 2 pasal 7)

Jakarta, 7 Maret 2014

Mahasiswa



RANGGA ADITYA SUTOPO, S.ST

NPM. 111.0921.053

**PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR/SKRIPSI/TESIS UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Rangga Aditya Sutopo, S.ST.
NPM : 111.0921.053
Fakultas : Pascasarjana
Program Studi : Magister Manajemen
Jenis Karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

**ANALISIS PENERAPAN KRIPTOGRAFI SEBAGAI SOLUSI KEAMANAN
INFORMASI PADA SISTEM INFORMASI PERENCANAAN DAN AKUNTABILITAS
KINERJA LEMBAGA SANDI NEGARA**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas Akhir/Skripsi/Tesis saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 7 Maret 2014

Yang Menyatakan,



Rangga Aditya Sutopo