



**PENGGABUNGAN ALGORITMA
KRIPTOGRAFI VERNAM DAN STEGANOGRAFI**

HERI SULISTIYO

41508110087

**UNIVERSITAS
MERCU BUANA**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2013



**PENGGABUNGAN ALGORITMA
KRIPTOGRAFI VERNAM DAN STEGANOGRAFI**

Laporan Tugas Akhir

Diajukan untuk melengkapi Salah Satu Syarat Memperoleh Gelar
Sarjana Strata Satu (1) Komputer

Oleh :

HERI SULISTIYO

41508110087

UNIVERSITAS
MERCU BUANA

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2013

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nim : 41508110087

Nama : HERI SULISTIYO

Judul Skripsi : **PENGGABUNGAN ALGORITMA
KRIPTOGRAFI VERNAM DAN STEGANOGRAFI**

Menyatakan bahwa skripsi tersebut diatas adalah hasil karya sastra saya sendiri dan bukan plagiat. Apabila ternyata ditemukan di dalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 27 Agustus 2013

UNIVERSITAS
MERCU BUANA



(HERI SULISTIYO)

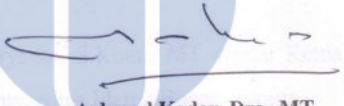
LEMBAR PENGESAHAN

Nim : 41508110087
Nama : HERI SULISTIYO
Judul Skripsi : **PENGABUNGAN ALGORITMA KRIPTOGRAFI
VERNAM DAN STEGANOGRAFI**

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI
SEBAGAI SYARAT MENGIKUTI SIDANG TUGAS AKHIR

Jakarta, 27 Agustus 2013

Menyetujui,


Achmad Kodar, Drs., MT

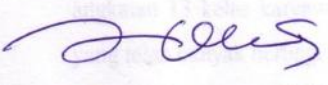
Pembimbing

UNIVERSITAS

MERCU BUANA

Mengetahui,

Mengesahkan,


Sabar Rudiarto, S.Kom., M.Kom
Koordinator Tugas Akhir
Teknik Informatika


Tri Daryanto, S.Kom., MT
Ketua Program Studi
Teknik Informatika

KATA PENGANTAR

Puji serta syukur kepada Allah SWT, atas berkat dan rahmat-Nya penulis dapat menyelesaikan tugas akhir ini yang berjudul **“PENGGABUNGAN ALGORITMA KRIPTOGRAFI VERNAM DAN STEGANOGRAFI “** serta shalawat beserta salam penulis haturkan kepada junjungan Nabi besar Muhammad SAW. Dimana tugas akhir ini merupakan bagian dari syarat mendapatkan gelar sarjana strata satu (S1) pada jurusan teknik informatika Universitas Mercu Buana.

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu, dimana dalam pengerjaan maupun dalam penulisan laporan tugas akhir ini banyak sekali hambatan dan kesulitan yang dialami oleh penulis. Pada kesempatan ini penulis mengucapkan terima kasih yang sebesar – besarnya kepada :

1. Bapak Achmad Kodar, Drs., MT selaku dosen pembimbing telah memberikan bimbingan dan sarannya dalam penulisan laporan tugas akhir ini.
2. Bapak Tri Daryanto, S.Kom., MT selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana, Jakarta.
3. Bapak Sabar Rudiarto, S.Kom., M.Kom selaku koordinator tugas akhir program studi Teknik Informatika, Universitas Mercu Buana, Jakarta.
4. Keluarga, Ibu tercinta yang tak henti – hentinya mengiringi penulis dengan do’a dan selalu memberikan semangat kepada penulis.
5. Semua mahasiswa/i Teknik Informatika khususnya teman –teman angkatan 13 kelas karyawan yang tidak bisa saya sebutkan satu persatu, yang telah banyak berbagi pengalaman, ilmu, dan juga semangat.
6. Semua pihak yang telah membantu baik langsung maupun tidak langsung.

Semoga Allah SWT. Memberikan rahmat dan balasan kepada mereka yang telah memberikan bantuan kepada penulis, dan tak lupa penulis mohon maaf kepada semua pihak atas kehilafan penulis selama menyelesaikan skripsi ini.

Meskipun penulis telah berusaha membuat tulisan ini semaksimal mungkin, namun penulis menyadari bahwa laporan ini tak luput dari kekurangan. Atas saran dan kritik yang membangun penulis mengucapkan terima kasih. Akhir kata semoga tulisan ini dapat memberikan manfaat bagi penulis khususnya dan pembaca pada umumnya.

Jakarta, 27 Agustus 2013

Penulis

Heri Sulistiyo



DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Metodologi Penelitian	3
1.5 Tujuan	3
1.6 Manfaat	3
1.7 Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1 Kriptografi	5
2.1.1 Definisi Kriptografi	5
2.1.2 Sejarah Kriptografi	6
2.1.3 Tujuan Kriptografi	8

2.1.4 Terminologi dan Konsep dasar Kriptografi	9
2.1.4.1 Pesan, Plainteks, dan Cipherteks	9
2.1.4.2 Peserta Komunikasi	10
2.1.4.3 Kriptologi	10
2.1.5 Algoritma dan Kunci	11
2.1.6 Jenis Algoritma Kriptografi	12
2.1.6.1 Algoritma Simetris	12
2.1.6.2 Algoritma Asimetris	13
2.1.7 Keamanan Sistem Kriptografi	15
2.1.7.1 Jenis-jenis Ancaman Keamanan	15
2.1.7.2 Serangan Pada Sistem Kriptografi	16
2.1.7.3 Kualitas Keamanan Algoritma	16
2.1.8 Algoritma Vernam Chiper	17
2.1.8.1 Pembangkit aliran-bit-kunci (Keystream Generator)...	19
2.1.8.2 Serangan Terhadap Cipher	21
2.1.8.3 Aplikasi Cipher	22
2.2 Steganografi	23
2.2.1 Definisi Steganografi	23
2.2.2 Algoritma LSB	24
2.2.3 Data Rate	26
2.2.3.1 Ketahanan	26
2.2.3.2 Solusi	26
2.3 UML (<i>Unified Modeling Language</i>)	27

2.3.1 Definisi UML	27
2.3.2 Use Case Diagram	27
2.3.3 Sequence Diagram	28
2.3.4 Activity Diagram	29
2.4 Java	32
2.5 Netbeans	36
BAB III ANALISIS DAN PERANCANGAN	37
3.1 Identifikasi Sistem	37
3.2 Analisis Kebutuhan Sistem	38
3.2.1 Diagram Use Case	38
3.2.2 Narasi Use Case	38
3.3 Perancangan Umum Sistem	40
3.3.1 Masukan Sistem	40
3.3.2 Proses Sistem	41
3.3.3 Keluaran Sistem	41
3.4 Diagram Aktifitas	42
3.4.1 Diagram Aktifitas Proses Steganografi dan Kriptografi.....	42
3.4.2 Diagram Aktifitas Ekstrak Stegano dan Kripto.....	43
3.5 Diagram Kelas Analisis	44
3.6 Sequence Diagram	44
3.7 Perancangan Antar Muka Sistem	45
BAB IV IMPLEMENTASI DAN PENGUJIAN	48
4.1 Perangkat Kebutuhan Sistem	48

4.2 Implementasi Antar Muka dengan Pengguna	48
BAB IV PENUTUP	59
5.1 Kesimpulan	59
5.2 Saran	59
DAFTAR PUSTAKA	60
LAMPIRAN	



DAFTAR GAMBAR

	Halaman
Gambar 2.1 Skema Kriptografi Simetri	13
Gambar 2.2. Skema Kriptografi Asimetri	14
Gambar 2.3 Konsep <i>cipher</i>	18
Gambar 2.4 <i>Cipher</i> aliran dengan pembangkit bit-aliran-kunci yang bergantung pada kunci <i>U</i>	20
Gambar 2.5 <i>Cipher</i> aliran dengan pembangkit bit-aliran-kunci yang bergantung pada kunci <i>U</i> dan umpan <i>Z</i>	21
Gambar 2.6 Aktor Menggunakan Use Case	28
Gambar 2.7 Objek, Garis Hidup, dan Aktivasi	29
Gambar 2.8 Simbol Pesan Dalam <i>Sequence Diagram</i>	29
Gambar 2.9 <i>activity diagram</i> dengan <i>swimlane</i>	31
Gambar 2.10 <i>activity diagram</i> tanpa <i>swimlane</i>	32
Gambar 3.1. Diagram Use Case	38
Gambar 3.2. Diagram Konteks	41
Gambar 3.3 Diagram Aktifitas Proses Steganografi dan Kriptografi	42
Gambar 3.4 Diagram Aktifitas Ekstraksi Steganografi dan Kriptografi	43
Gambar 3.5 Diagram kelas Analisis Proses Steganografi dan Kriptografi	44
Gambar 3.6 Diagram Sequence pada aplikasi penggabungan kriptografi dan steganografi	45
Gambar 3.7 Perancangan Halaman Utama Aplikasi	45
Gambar 3.8 Perancangan Menu Aplikasi	46
Gambar 3.9 Perancangan Menu Stegano & Kriptografi	46
Gambar 3.10 Perancangan Ekstraksi Steganografi dan Kriptografi	46

Gambar 3.11 Perancangan About	47
Gambar3.12 Perancangan Help	47
Gambar 4.1 Halaman Utama	48
Gambar 4.2 Halaman Stegano&Kripto	50
Gambar 4.3 Penginputan Picture	50
Gambar 4.4 Hasil Penginputan untuk proses Stegano dan kripto	51
Gambar 4.5 Sample data a.txt	51
Gambar 4.6 Penginputan Stegano dan Crypto	52
Gambar 4.7 Konfirmasi berhasil proses Stegano dan Kripto	52
Gambar 4.8 Hasil File gambar dan File key	53
Gambar 4.9 Hasil File Key	53
Gambar 4.10 Halaman Ekstrak	54
Gambar 4.11 file image yang akan di proses	54
Gambar 4.12 Memilih File key	55
Gambar 4.13 Hasil Penginputan nama file yang akan di ekstrak	55
Gambar 4.14 Informasi gambar tidak ada file yang di hidden	56
Gambar 4.15 Informasi Berhasil Ekstrak	56
Gambar 4.16 Hasil Ekstraksi pada Windows Explorer	57
Gambar 4.17 Hasil Ekstrasi File Hidden	57
Gambar 4.18 Halaman Menu About	58
Gambar 4.19 Halaman Menu Help	58

DAFTAR TABEL

	Halaman
Tabel 2.1. Batas nilai floating point	34

