

**HYBRID KRIPTOGRAFI - STEGANOGRAFI MENGGUNAKAN
VERNAM CIPHER, VIGENERE CIPHER, DAN LSB PADA
PENGIRIMAN PESAN RAHASIA**

SKRIPSI



**disusun oleh
Muh. Hutomo Perdana Putra
14.11.8433**

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**

**HYBRID KRIPTOGRAFI - STEGANOGRAFI MENGGUNAKAN
VERNAM CIPHER, VIGENERE CIPHER, DAN LSB PADA
PENGIRIMAN PESAN RAHASIA**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Muh. Hutomo Perdana Putra

14.11.8433

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**

PERSETUJUAN

SKRIPSI

**HYBRID KRIPTOGRAFI - STEGANOGRAFI MENGGUNAKAN
VERNAM CIPHER, VIGENERE CIPHER, DAN LSB PADA
PENGIRIMAN PESAN RAHASIA**

yang dipersiapkan dan disusun oleh

Muh Hutomo Perdana Putra

14.11.8433

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 7 Mei 2018

Dosen Pembimbing,

Rizqi Sukma Kharisma, M.Kom
NIK. 190302215

PENGESAHAN

SKRIPSI




**HYBRID KRIPTOGRAFI - STEGANOGRAFI MENGGUNAKAN
VERNAM CIPHER, VIGENERE CIPHER, DAN LSB PADA
PENGIRIMAN PESAN RAHASIA**

yang dipersiapkan dan disusun oleh

Muh Hutomo Perdana Putra
14.11.8433

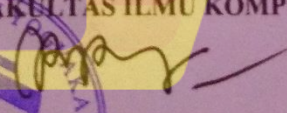
telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Mei 2018


Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
<u>Ali Mustopa, M.Kom</u> NIK. 190302192	
<u>Donni Prabowo, M.Kom</u> NIK. 190302353	
<u>Rizqi Sukma Kharisma, M.Kom</u> NIK. 190302215	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 7 Juni 2018

DEKAN FAKULTAS ILMU KOMPUTER


Krisnawati, S.Si, M.T.
NIK. 190302038



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, 03-06-2018



Muh. Hutomo Perdana Putra

NIM. 14.11.8433

MOTTO

”You can’t change the choice you made, all you can do is not let it ruin you”

- Akabane Karma –

”Life doesn't give us purpose, we give life purpose”

- Barry Allen –

” Pendidikan merupakan perlengkapan paling baik untuk hari tua”

- Aristoteles -

” Tugas kita bukanlan untuk berhasil. Tugas kita adalah untuk mencoba, karena di dalam mencoba itulah kita menemukan dan membangun kesempatan untuk berhasil”

- Mario Teguh –

” Learn from yesterday,

Live for today,

And hope for tomorrow”

- Albert Einstein -

PERSEMBAHAN

Dengan rasa bangga dan bahagia saya khaturkan rasa syukur dan terima kasih saya kepada :

1. Allah Subhanahu wa ta'ala, karena atas izin dan karunia-Nya maka skripsi ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada-Nya sebagai penguasa alam yang mengabulkan segala do'a.
2. Bapak dan Ibu saya yang telah memberikan dukungan moral maupun materi serta do'a yang tiada henti untuk kesuksesan saya, karena tiada kata seindah lantunan do'a dan tiada do'a yang paling khusuk selain do'a yang terucap dari orang tua.
5. Keluarga Besar dari Ibu dan Bapak yang berada di Makassar, Sorong, dan Majene yang sudah memberikan dukungan, semangat dan motivasi kepada saya.
6. Teman – teman kelas “14 S1 TI 14” sekarang berubah menjadi “14 S1 IF 14” yang sudah memberikan dukungan, semangat dan motivasi meskipun kita sering becanda dikelas tapi rasa cinta kita ke sesama begitu besar. Semoga kita selalu dalam lindungan-Nya dan diberikan kebahagiaan serta kesuksesan dunia akhirat.
7. Untuk mereka, sahabat-sahabat saya dari TI-14 terima kasih karna kalian selalu bisa menerima saya dengan sabar, dan selalu membatu saya, Odhier, Levi, Fitri, Mameh, Febri, Adhima, Rexy, Entong, Dan seluruh teman-teman TI-14, Semoga kita dapat dipertemukan kembali dalam sukses yang selalu kita rencanakan
8. Dan untuk yang selalu men-supportku selama membuat skripsi ini yang selalu memberiku *asupan mood booster* sebagai penyemangat☺.

KATA PENGANTAR

Puji dan syukur kehadirat Allah subhanahu wa ta'ala atas seluruh nikmat yang masih Ia berikan hingga detik ini, tak lupa pula shalawat kepada nabi besar junjungan seluruh umat Muhammad shallallahu alaihi wa sallam yang semoga pada akhir dari cerita kita di dunia ini kita dapat melihatnya walau dari kejauhan di syurgaNya Allah.

Skripsi ini merupakan bagian dari syarat utama yang harus dipenuhi untuk mencapai jenjang Sarjana Komputer pada kampus terpadu Universitas Amikom Yogyakarta. Atas terselesaikannya penulisan skripsi ini maka penulis ingin berterima kasih kepada :

1. Prof. Dr. M. Suyanto, MM. Sebagai rektor dari Universitas Amikom Yogyakarta.
2. Bapak Rizqi Sukma Kharisma, M.Kom. sebagai pembimbing saya dalam proses penulisan skripsi ini.
3. Bapak Ali Mustopa, M.Kom dan Bapak Donni Prabowo, M.Kom selaku penguji pada ujian skripsi saya.
4. Seluruh Dosen Universitas Amikom Yogyakarta yang telah membagikan ilmunya kepada saya.

Yogyakarta, 03 Juni 2018

Penulis

DAFTAR ISI

JUDUL	ii
PERSETUJAN	iii
PENGESAHAN	iv
PERNYATAAN.....	v
MOTTO.....	vi
PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
INTISARI.....	xv
<i>ABSTRACT</i>	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
1.6 Metode Penelitian.....	3
1.7 Sistematika Penelitian	4
BAB II LANDASAN TEORI	6
2.1 Tinjauan Pustaka	6
2.2 Kriptografi	8
2.2.1 Definisi Kriptografi.....	8
2.2.2 Tujuan Kriptografi	10
2.2.3 Jenis – jenis Algoritma Kriptografi.....	11
2.3 Algoritma Kriptografi.....	14
2.3.1 Vigenere Cipher	14
2.3.2 Vernam Cipher.....	18
2.3 Steganografi.....	20

2.4.	Algoritma Steganografi	21
2.4.1	<i>Least Significant Bit (LSB)</i>	23
2.5	<i>Website</i>	24
2.5.1	Pemrograman <i>Website</i>	24
2.6	<i>Software</i> yang digunakan	26
2.6.1	Sublime Text 3	26
2.6.2	<i>Website Browser</i>	27
2.6.3	Web Server.....	28
2.7	Bahasa Pemrograman	29
2.7.1	HTML (Hypertext Markup Language)	29
2.7.2	PHP (Hypertext Preprocessor)	29
2.7.3	SQL (Structured Query Language)	30
2.8	Metode Pengembangan	30
2.8.1	<i>Waterfall</i>	30
2.9	Analisis Sistem	32
2.9.1	Defenisi Analisis Sistem	32
2.9.2	Analisis SWOT	32
2.9.3	Analisis Kebutuhan Sistem	34
2.9.4	Analisis Kelayakan Sistem.....	34
2.10	Pemodelan Sistem.....	35
2.10.1	<i>Entity Relation Diagram (ERD)</i>	35
2.10.2	<i>Use Case</i>	36
2.10.3	<i>Class Diagram</i>	37
2.10.4	<i>Activity Diagram</i>	38
BAB III ANALISIS DAN PERANCANGAN SISTEM		38
3.1	Gambaran Aplikasi.....	38
3.1.1	Pengiriman Pesan (Enkripsi).....	39
3.1.2	Penerjemah Pesan (Dekripsi)	39
3.2	Analisis	40
3.2.1	Analisis SWOT	40
3.2.2	Analisis Kebutuhan	41
3.3	Kelayakan Sistem	44

3.3.1	Kelayakan Teknologi	44
3.3.2	Kelayakan Operasional	44
3.3.3	Kelayakan Hukum.....	44
3.4	Perancangan.....	45
3.4.1	Perancangan Sistem	45
3.4.2	Perancangan Database.....	51
3.4.3	Perancangan User Interfaces	53
BAB IV IMPLEMENTASI DAN PEMBAHASAN		58
4.1	Implementasi	58
4.2	Pembahasan Database	58
4.3	Pembahasan <i>Interfaces</i>	59
4.4	Pengujian Sistem	74
4.4.1	Pengujian Penyisipan Pesan	74
4.4.3	Pengujian Dekripsi Pesan.....	79
4.4.4	<i>White Box Testing</i>	79
4.4.5	<i>Black Box Testing</i>	80
4.5	Manual Program	81
BAB V PENUTUP.....		85
5.1	Kesimpulan.....	85
5.2	Saran	86
DAFTAR PUSTAKA		87

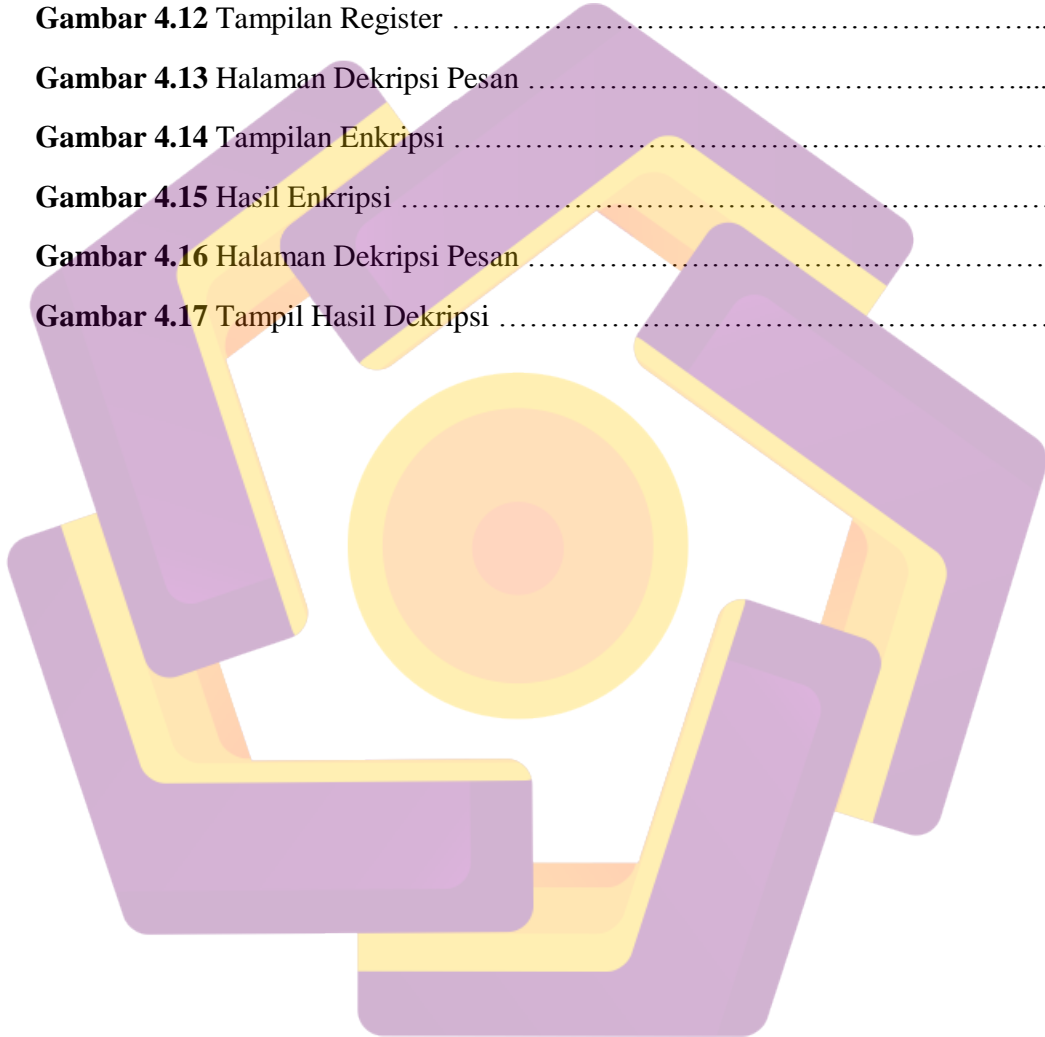
DAFTAR TABEL

Tabel 2.1 Tabel penukaran huruf ke angka	14
Tabel 2.2 Tabel proses penukaran dan hasil ciphertext	14
Tabel 2.3 Tabel Bujur-Sangkar Vigenere	15
Tabel 2.4 Enkripsi Huruf J (Plainteks) dengan Huruf K (Kunci)	16
Tabel 2.5 Tabel Bujur-Sangkar Vigenere	18
Tabel 2.6 Enkripsi Huruf J (Plainteks) dengan Huruf I (Kunci)	19
Tabel 2.7 Simbol-simbol ERD (<i>Entity Relation Diagram</i>)	34
Tabel 2.8 Simbol-simbol <i>Use Case Diagram</i>	34
Tabel 2.9 Simbol-simbol <i>Class Diagram</i>	35
Tabel 2.10 Simbol-simbol <i>Activity Diagram</i>	36
Tabel 3.1 Spesifikasi Hardware	43
Tabel 3.2 Spesifikasi <i>Software</i>	43
Tabel 3.3 Tabel <i>user</i>	52
Tabel 3.4 Tabel <i>encrypt_histories</i>	52
Tabel 3.5 Tabel <i>decrypt_histories</i>	53
Tabel 4.1 Tabel uji penyisipan pesan (<i>encrypt</i>)	75
Tabel 4.2 Tabel uji ekstrak pesan yang ada didalam gambar (<i>decrypt</i>)	79
Tabel 4.3 Hasil Pengujian <i>Black Box Testing</i>	80

DAFTAR GAMBAR

Gambar 2.1 Skema Enkripsi Dan Dekripsi Menggunakan Kunci	10
Gambar 2.2 Skema Algoritma Simetris	12
Gambar 2.3 Skema Algoritma Asimetris	13
Gambar 2.4 <i>Software</i> Sublime Text 3	25
Gambar 2.5 <i>Browser</i> Google Chrome	25
Gambar 2.6 <i>Software</i> XAMPP control panel	27
Gambar 2.7 <i>Waterfall model</i>	29
Gambar 3.1 <i>Flowchart</i> Aplikasi V2L	45
Gambar 3.2 <i>Flowchart</i> Metode	46
Gambar 3.3 <i>Use Case</i> Diagram	47
Gambar 3.4 <i>Activity Diagram</i> Encryption Message	48
Gambar 3.5 <i>Activity Diagram</i> Decryption Message	49
Gambar 3.6 <i>Activity Diagram</i> Login	50
Gambar 3.7 <i>Activity Diagram</i> Registrasi	50
Gambar 3.8 Entity Relation Diagram	51
Gambar 3.9 Tabel Relasi	52
Gambar 3.10 Halaman Enkripsi	54
Gambar 3.11 Halaman Dekripsi	55
Gambar 3.12 Halaman <i>About</i>	55
Gambar 3.13 Halaman <i>Login</i>	56
Gambar 3.14 Halaman Registrasi	56
Gambar 3.15 Halaman <i>History</i>	57
Gambar 4.1 Tabel <i>Users</i>	58
Gambar 4.2 Tabel <i>history encryption</i>	59
Gambar 4.3 Tabel <i>history decryption</i>	59
Gambar 4.4 <i>Interface</i> Halaman Enkripsi	60
Gambar 4.5 <i>Interface</i> Halaman Dekripsi	67
Gambar 4.6 Halaman <i>Register</i>	70

Gambar 4.7 Halaman <i>Login</i>	71
Gambar 4.8 <i>file image</i> sebelum dan sesudah disisipkan pesan rahasia	77
Gambar 4.9 <i>Histogram</i> warna RGB sebelum dan sesudah disisipkan pesan	78
Gambar 4.10 Pesan <i>error</i> ukuran gambar minimal 400x400	80
Gambar 4.11 Tampilan <i>home website</i> V2L	81
Gambar 4.12 Tampilan Register	82
Gambar 4.13 Halaman Dekripsi Pesan	82
Gambar 4.14 Tampilan Enkripsi	83
Gambar 4.15 Hasil Enkripsi	83
Gambar 4.16 Halaman Dekripsi Pesan	84
Gambar 4.17 Tampil Hasil Dekripsi	84



INTISARI

Perkembangan ilmu pengetahuan sangat berpengaruh pada perkembangan dunia teknologi. Salah satu teknologi yang sedang berkembang adalah teknologi informasi yang dimana dengan kemudahan untuk mencari suatu informasi dengan cepat tanpa harus memperhatikan batasan ruang dan waktu sehingga dalam hitungan menit, kita dapat mengetahui informasi suatu negara. Akan menjadi sebuah kerugian jika suatu informasi yang dianggap rahasia dapat diketahui oleh pihak lain, maka dari itu untuk merahasiakan suatu pesan dibutuhkan teknik enkripsi kriptografi dan Steganografi.

Kriptografi, ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi. Steganografi adalah proses menyimpan pesan rahasia berupa teks dalam bentuk lain sehingga tidak mudah diketahui oleh orang lain. Berbagai macam steganografi antara lain menyembunyikan pesan ke dalam file gambar, file audio, dan file video.

Algoritma Vigenere dan Vernam merupakan algoritma yang dipilih untuk merancang suatu aplikasi yang memungkinkan untuk melakukan enkripsi kriptografi terhadap pesan dan Algoritma LSB merupakan algoritma yang dipilih untuk menyisipkan hasil pesan enkripsi Kripto ke dalam file citra gambar.

Kata Kunci : Kriptografi, Steganografi, Vigenere, Vernam, LSB.

ABSTRACT

The development of science is very influential on the progress of the world of technology. One of the emerging technologies is technology of information where the simplicity of finding the information quickly without concern on the limitation of the space and period, so that, in only a minute we are able to know the country's information. It would be a disadvantage if any information that is considered as a confidential information can be known by any parties, therefore to keep it save, a cryptographic and steganographic encryption technique is required.

Cryptography, science and art to maintain the security of messages when messages are sent from one place to another that relies on mathematical techniques for dealing with information security. Steganography is the process of storing secret messages in the form of text in other forms so it is not easily known by others. Various kinds of steganography include hiding messages into image files, audio files, and video files.

The Vigenere and Vernam algorithms are the chosen algorithm to design an application that allows for cryptographic to encrypt the messages and the LSB algorithm is the chosen algorithm to insert the results of Crypto encryption messages into image files.

Keyword : Cryptography, Steganography, Vigenere, Vernam, LSB.