

**IMPLEMENTASI STEGANOGRFI DENGAN PENGGABUNGAN
KRIPTOGRAFI METODE VINEGERE DAN
CAESAR SUBSITUTION**

SKRIPSI



disusun oleh

CICIK KUSUMAWARDANI

04.11.0514

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
YOGYAKARTA**

2010

**IMPLEMENTASI STEGANOGRFI DENGAN PENGGABUNGAN
KRIPTOGRAFI METODE VINEGERE DAN
CAESAR SUBSTITUTION**

Skripsi

untuk memenuhi sebagian persyaratan mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

CICIK KUSUMAWARDANI

04.11.0514

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
YOGYAKARTA**

2010

PERSETUJUAN

SKRIPSI

IMPLEMENTASI STEGANOGRFI DENGAN PENGGABUNGAN
KRIPTOGRAFI METODE VINEGERE DAN
CAESAR SUBSITUTION

yang dipersiapkan dan di susun oleh

Cicik kusumawardani

04.11.0514

Telah disetujui oleh Dosen Pembimbing Skripsi
Pada tanggal 19 Oktober 2010

Dosen Pembimbing,


Dr. Ema Utami, S.Si., M.Kom

NIK. 190302037

PENGESAHAN

SKRIPSI

**IMPLEMENTASI STEGANOGRFI DENGAN PENGGABUNGAN
KRIPTOGRAFI METODE VINEGERE DAN
CAESAR SUBSITUTION**

yang dipersiapkan dan di susun oleh

Cicik kusumawardani

04.11.0514

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 19 Oktober 2010

Susunan Dewan Penguji

Nama Penguji

**Armadyah Amborowati, S.Kom., M.Eng.
NIK. 190302063**

**Dr. Ema Utami, S.Si, M.Kom.
NIK. 190302037**

**Kusnawi, S.Kom., M.Eng.
NIK. 190302112**

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Oktober 2010

KETUA STM IK AMIKOM YOGYAKARTA



**Prof. Dr. M. Suvanto, M.M.
NIK. 190302001**

PERNYATAAN KEASLIAN

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, 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.

Yogyakarta, 19 Oktober 2010



Cicik Kusumawardani
04.11.0514

Motto

Sempurnakan segala sesuatu yang baik itu dengan niat, usaha dan do'a

Niscaya ALLAH akan membantumu ...



KATA PENGANTAR



Assalamu'alaikum Wr. Wb.

Dengan mengucapkan puji dan syukur kehadirat Allah S.W.T. yang telah melimpahkan Rahmat dan Hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul ” **IMPLEMENTASI STEGANOGRFI DENGAN PENGGABUNGAN KRIPTOGRAFI METODE VINEGERE DAN CAESAR SUBSITUTION**” sebagai salah satu persyaratan untuk menyelesaikan program studi strata-1 Jurusan Teknik Informatika di STMIK “AMIKOM” Yogyakarta.

Skripsi ini dapat diselesaikan berkat saran, bimbingan, motifasi, dorongan dan kerjasamanya dari berbagai pihak, maka pada kesempatan ini penulis ingin mengucapkan rasa terimakasih kepada pihak-pihak yang telah membantu penulis. Oleh karena itu penulis mengucapkan terimakasih yang sebesar-besarnya kepada yang terhormat :

1. Bapak Prof. Dr. Mohammad Suyanto, M.M. Selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer STMIK ‘AMIKOM’ Yogyakarta.
2. Ibu Ema Utami, Dr., M.Kom selaku dosen pembimbing, terima kasih atas masukannya selama bimbingannya.
3. Ibunda tercinta, terimakasih atas motivasi dan perhatiannya, semoga Allah selalu memberikan kesehatan jasmani dan rohani.

4. Kakak dan adik-ku yang tercinta, terima kasih atas dukungannya dan motivasinya.
5. Irman orang yang sangat berarti buat ku, Terima kasih atas bantuan dan perhatiannya selama ini.
6. Akmal, Putri, Wahyus (ncus), Sari, dan Reza. Terima kasih atas semua bantuannya.
7. Semua teman-teman Informatika '04, semua dosen Teknik Informatika, semua kakak – kakak dan adik – adik tingkat terima kasih atas semuanya.
8. Serta semua pihak yang tidak bisa disebutkan satu persatu.

Semoga Allah SWT, memberikan rahmat yang berlipat ganda atas amal dan bantuan yang diberikan kepada penulis sehingga apa yang dicita-citakan dapat tercapai sesuai dengan yang direncanakan. Amin.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 19 Oktober 2010

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN	iv
HALAMAN MOTO DAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR GRAFIK	xv
DAFTAR ALGORITMA	xvi
INTISARI	xvii
ABSTRACT	xviii
BAB I PENDAHULUAN	
1.1 LATAR BELAKANG MASALAH	1
1.2 RUMUSAN MASALAH	5
1.3 BATASAN MASALAH	5
1.4 TUJUAN PENELITIAN.....	6
1.5 MANFAAT PENELITIAN	6
1.6 METODE PENELITIAN	6

1.7 SISTEMATIKA PENULISAN.....	7
--------------------------------	---

BAB II LANDASAN TEORI

2.1 TINJAUAN PUSTAKA.....	8
---------------------------	---

2.2 KRIPTOGRAFI	9
-----------------------	---

2.2.1 Pengertian dan Testimoni Kriptografi	9
--	---

2.2.2 Sejarah Kriptografi	10
---------------------------------	----

2.2.3 Algoritma Kriptografi	10
-----------------------------------	----

2.3 <i>VENEGERE CHIPTER</i>	13
-----------------------------------	----

2.4 <i>CAESAR CHIPTER</i>	17
---------------------------------	----

2.5 <i>STEGANOGRAFI</i>	18
-------------------------------	----

2.5.1 Pengertian dan Testimoni Kriptografi	18
--	----

2.5.2 Sejarah Kriptografi	19
---------------------------------	----

2.5.3 Tehnik Kriptografi	20
--------------------------------	----

2.6 METODE LSB (LEST SIGNIFICANT BIT)	22
---	----

2.7 CITRA DIGITAL	24
-------------------------	----

2.7.1 Pengertian Citra Digital	24
--------------------------------------	----

2.7.2 Citra dalam Format <i>Bitamp</i> (BMP)	25
--	----

2.8 BORLAND DELPHI	26
--------------------------	----

2.8.1 Pengantar Borland Delphi	26
--------------------------------------	----

2.8.2 Dasar Pemograman Borland Delphi	31
---	----

2.9 KONSEP DASAR PERANGKAT LUNAK	34
--	----

2.9.1 Pengertian Perangkat Lunak	34
2.9.2 Perancangan dan Pengembangan Perangkat Lunak	34
2.10 DATA FLOW DIAGRAM (DFD)	37
2.10.1 Terminator / Entitas Luar	38
2.10.2 Komponen Proses	39
2.10.3 Komponen Data Store	39
2.10.4 Alur Data	40
2.10.5 Aturan Pembuatan DFD	42
BAB III ANALISIS DAN PERANCANGAN SISTEM	
3.1 ANALISA PERANCANGAN SISTEM	43
3.1.1 Kebutuhan Perangkat Lunak	43
3.1.2 Strategi Perancangan Perangkat Lunak	44
3.2 PERANCANGAN	46
3.2.1 Perancangan Flowchat	46
3.2.2 Perancangan Diagram Konteks	47
3.2.3 Perancangan Diagram DFD	48
3.2.3.1 DFD level 0	49
3.2.3.2 DFD Level 1 proses Write message	50
3.2.3.3 DFD Level 1 proses Read message	51
3.2.4 Perancangan Antarmuka (Interface)	52
3.2.5 Perancangan Script Program	55

BAB IV IMPLEMENTASI DAN UJI COBA

4.1 IMPLEMENTASI SISTEM	63
4.1.1 Menu Panduan	63
4.1.2 Menu Enkripsi	65
4.1.3 Menu Dekripsi	69
4.2 KESALAHAN-KESALAHAN PROGRAM	72
4.3 SIMULASI UJI COBA PROGRAM DAN HASIL	73
4.3.1 Pengujian Enkripsi menggunakan metode venegere	73
4.3.2 Pengujian Enkripsi menggunakan metode Caesar	74
4.3.3 Pengujian steganografi pada gambar berekstensi *.bmp ...	75
4.3.4 Pengujian Dekripsi menggunakan metode Caesar	77
4.3.5 Pengujian Dekripsi menggunakan metode venegere	78
4.4 PEMBAHASAN MASALAH	79
4.4.1 Cara Kerja Kinerja Sistem	79
4.4.2 Kelebihan Sistem.....	79
4.4.3 Kekurangan Sistem	80
4.5 PENGUJIAN TINGKAT KEBERHASILAN	80

BAB V KESIMPULAN DAN SARAN

5.1 KESIMPULAN	84
5.2 SARAN	85

DAFTAR PUSTAKA	xix
----------------------	-----

LAMPIRAN

DAFTAR TABEL

Tabel 2.1. Tabel Vinegere.....	14
Tabel 4.2. Tabel uji coba program	81



DAFTAR GAMBAR

Gambar 2.1. Gambar kriptografi kunci simetris	11
Gambar 2.2. Gambar kriptografi kunci asimetris	11
Gambar 2.3a. Gambar skema enkripsi dan dekripsi	12
Gambar 2.3b. Gambar ilustrasi enkripsi dan dekripsi	12
Gambar 2.4. Gambar proses steganografi	22
Gambar 2.5. Gambar tampilan lingkungan kerja delphi	27
Gambar 2.6. Gambar tampilan form pada delphi.....	27
Gambar 2.7. Gambar tampilan komponen delphi	28
Gambar 2.8. Gambar tampilan object inspector.....	28
Gambar 2.9. Gambar tampilan object tree view	29
Gambar 2.10. Gambar tampilan code editor	29
Gambar 2.11. Gambar tampilan menu bar	30
Gambar 2.12. Gambar tool bar.....	30
Gambar 2.13. Gambar model proses.....	34
Gambar 2.14. Gambar waterfall model.....	35
Gambar 2.15. Gambar DFD menurut Yourdan dan Marco	37
Gambar 2.16. Gambar DFD menurut Gene dan serson	37
Gambar 2.17. Gambar terminator atau entitas luar	37
Gambar 2.18. Gambar komponen proses	38
Gambar 2.19. Gambar komponen data store.....	40
Gambar 2.20. Gambar pocket of data	40
Gambar 2.21. Gambar konsep diverging data flow	41
Gambar 2.22. Gambar konsep converging data flow.....	41
Gambar 2.23. Gambar konsep sumber dan tujuan	41
Gambar 3.24. Gambar bagan perencanaan	45
Gambar 3.25. Gambar flowchart sistem keamanan data.....	46
Gambar 3.26. Gambar diagram konteks	48
Gambar 3.27. Gambar DFD level 0	49
Gambar 3.28. Gambar DFD level 1 proses embedding	50
Gambar 3.29. Gambar DFD level 1 proses ekstraksi.....	51

Gambar 3.30. Gambar form enkripsi	52
Gambar 3.31. Gambar form deskripsi.....	53
Gambar 3.32. Gambar form panduan.....	54
Gambar 4.33. Gambar menu panduan.....	64
Gambar 4.34. Gambar tampilan ganti skin	65
Gambar 4.35. Gambar tampilan menu panduan.....	65
Gambar 4.36. Gambar tampilan menu enkripsi	66
Gambar 4.37. Gambar tampilan image asli.....	66
Gambar 4.38. Gambar tampilan enkripsi yang belum disisipkan pesan	67
Gambar 4.39. Gambar tampilan info cek gambar	67
Gambar 4.40. Gambar tampilan enkripsi vinegere	68
Gambar 4.41. Gambar tampilan enkripsi caesar	68
Gambar 4.42. Gambar tampilan enkripsi yang di simpan.....	69
Gambar 4.43. Gambar info spesifikasi data enkripsi	69
Gambar 4.44. Gambar tampilan dekripsi	70
Gambar 4.45. Gambar tampilan menu dekripsi	70
Gambar 4.46. Gambar tampilan gambar yang didekripsikan	71
Gambar 4.47. Gambar tampilan gambar yang akan didekripsikan	71
Gambar 4.48. Gambar tampilan dekripsi caesar	72
Gambar 4.49. Gambar tampilan dekripsi vinegere	72
Gambar 4.50. Gambar data spesifikasi dekripsi	73
Gambar 4.51. Gambar tampilan enkripsi metode vinegere.....	74
Gambar 4.52. Gambar tampilan chiperteks.....	75
Gambar 4.53. Gambar tampilan enkripsi caesar	75
Gambar 4.54. Gambar tampilan file.bmp.....	76
Gambar 4.55. Gambar tampilan umum file .bmp	76
Gambar 4.56. Gambar tampilan file yang telah disisipkan.....	77
Gambar 4.57. Gambar tampilan umum file yang telah disisipkan.....	77
Gambar 4.58. Gambar tampilan chiperteks	78
Gambar 4.59. Gambar tampilan hasil enkripsi caesar	79
Gambar 4.60. Gambar dekripsi vinegere	79

DAFTAR GRAFIK

Grafik 4.1. Grafik kecepatan proses enkripsi dan dekripsi	82
Grafik 4.2. Grafik perbandingan ukuran file.....	83



DAFTAR ALGORITMA

Algoritma 3.1. Algoritma function biner	55
Algoritma 3.2. Algoritma function biner 16	56
Algoritma 3.3. Algoritma pangkat	56
Algoritma 3.4. Algoritma desimal	57
Algoritma 3.5. Algoritma WriteMessage	60
Algoritma 3.6. Algoritma extracting	61
Algoritma 3.7. Algoritma enkripsi vinegere	62
Algoritma 3.8. Algoritma dekripsi vinegere	62
Algoritma 3.9. Algoritma enkripsi caesar	63
Algoritma 3.10. Algoritma dekripsi caesar	63

INTISARI

Keamanan data sangat diperlukan untuk menjaga data yang penting dan rahasia. Salah satu metode yang digunakan adalah teknik penyandian data, yang di kenal dengan ilmu kriptografi. Dengan teknik ini data asli disandikan atau di enkripsi menjadi data rahasia sehingga data itu tidak akan berarti apa-apa bagi pihak yang tidak berwenang yang berhasil mengakses aset atau informasi. Diantara metode algoritma kriptografi yang pakai adalah algoritma vinegere dan caesar substitution.

Penelitian keamanan data yang dimaksud didalam judul menggabungkan algoritma vinegere dan caesar substitution menggunakan metode LBS menjadi suatu aplikasi yang saling menguatkan untuk mengamankan *file* txt dimana *file* txt sebagai data asli di enkripsi dengan vinegere dan setelah itu di enkripsi kembali dengan metode caesar. Penelitian ini dilakukan dengan cara mengumpulkan informasi dengan metode kepustakaan, metode dokumentasi dan metode observasi. Setelah informasi yang dibutuhkan didapat, maka selanjutnya dilakukan analisa data dan kebutuhan sistem. Setelah tahap analisa selesai dilanjutkan dengan perancangan aplikasi yang terdiri dari perancangan diagram konteks, perancangan DFD (*data flow diagram*), perancangan *flowchart* dan perancangan antarmuka. Setelah tahap perancangan selesai diteruskan ke implementasi program kemudian dilakukan pengujian program.

Hasil dari penelitian ini adalah suatu aplikasi keamanan data menggunakan algoritma vinegere dan caesar substitution. Aplikasi ini mampu mengenkripsi *file* teks yang berekstensi txt. Hasil pengujian tingkat keberhasilan enkripsi dan dekripsi dari aplikasi ini diperoleh persentase sebesar 100% sesuai dengan yang diharapkan. Berdasarkan pengujian program dapat disimpulkan bahwa aplikasi ini bermanfaat dan berguna untuk menjaga keamanan data *file* .txt.

Kata-kunci : Kriptografi, vinegere, caesar

ABSTRACT

Data security is very necessary to maintain a critical and confidential data. One method used is data encryption techniques, which in the know with the science of cryptography. In this way the original data is encoded or the encryption to confidential data so that data will not be meaningful to an unauthorized person who managed to access the assets or information. Among the methods that use cryptographic algorithms are the algorithm vinegere and caesar substitution.

Research data security is a title in the combined algorithm and caesar substitution vinegere LBS method into an application is mutually beneficial to secure the txt file where the txt file as the original data encrypted with vinegere and after that the encryption back to the methods section. This research was conducted by collecting information with literature methods, methods of documentation and observation methods. Following information were obtained, we then conducted data analysis and system requirements. After the analysis phase is completed followed by a design which consists of designing application context diagram, DFD design (data flow diagrams), design flowchart and interface design. After the design phase is completed and then forwarded to the implementation of program testing program.

The results of this study is a security application data using algorithms vinegere and caesar substitution. This application is able to encrypt a txt text file. Results of testing the success rate of encryption and decryption of the application obtained by the percentage of 100% as expected. Based on the testing program can be concluded that this application useful and handy to keep your data secure files. Txt.

Keywords : cryptographic, vinegere, caesar