ANALISIS DAN IMPLEMENTASI ENKRIPSI BASIS DATA DENGAN ALGORTIMA KRIPTOGRAFI BLOWFISH

SKRIPSI

disusun oleh

Ari Suhendra

06.11.1120

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2012

ANALISIS DAN IMPLEMENTASI ENKRIPSI BASIS DATA DENGAN ALGORTIMA KRIPTOGRAFI BLOWFISH

Skripsi

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

disusun oleh

Ari Suhendra

06.11.1120

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2012

PERSETUJUAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI ENKRIPSI BASIS DATA DENGAN ALGORTIMA KRIPTOGRAFI BLOWFISH

yang dipersiapkan dan disusun oleh

Ari Suhendra

06.11.1120

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 18 Januari 2011

Dosen Pembimbing,

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

PENGESAHAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI ENKRIPSI BASIS DATA DENGAN ALGORTIMA KRIPTOGRAFI BLOWFISH

yang dipersiapkan dan disusun oleh

Ari Suhendra

06.11.1120

telah dipertahankan di depan Dewan Penguji
pada tanggal 15 juni 2012

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dr. Ema Utami, S.si, M.Kom. NIK.190302037	
Dhani Ariatmanto, M.Kom. NIK. 190302197	
Tonny Hidayat, Mkom. NIK. 190302182	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 15 juni 2012

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Dengan ini saya menyatakan bahwa penelitian yang saya lakukan adalah hasil karya sendiri. Tidak ada karya ilmia atau sejenisnya yang di ajukan untuk memperoleh gelar kesarjanaan atau sejenisnya di perguruan tinggi manapun seperti karya ilmiah yang saya susun.

Sepengetahuan saya juga, tidak ada karya ilmia atau pendapat yang pernah ditulis atau di terbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah karya ilmia yang saya susun ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 1 agustus 2012

Ari Suhendra

MOTTO

Ceroboh dan tidak bisa menahan emosi adalah sikap yang bisa berakibat fatal.

Kejarlah duniamu seakan kamu hidup selamanya dan kejarlah akhiratmu seakan kamu mati besok.

Harapan kosong itu lebih menyakitkan dari pada kenyataan yang pahit sekalipun.

Setiap pekerjaan dapat diselesaikan dengan mudah bila dikerjakan tanpa keenganan, jangan tundah sampai besok apa yang bias engkau kerjakan hari ini.

Kegagalah hanya terjadi bila kita menyerah - ***Lessing***

Saya dating, saya bimbingan, saya ujian saya revisi dan saya menang.

PERSEMBAHAN

Thank's To:

- Allah SWT yang telah memberikan ridhoNya sehingga skripsi ini dapat terselesaikan.
- Ayah dan ibu tercinta, motivator terbesar dalam hidupku yang tak pernah jemu mendo'akan dan menyayangiku, atas semua pengorbanan dan kesabaran mengantarku sampai kini. Tak pernah cukup ku membalas cinta ayah dan ibu.
- Kedua kakak ku, Benni Marta dan Elan Saputra yang selalu memberiku semangat.
- Keluarga besarku yang selalu memberikan support sehingga aku dapat melaksanakan perkuliahan hingga penyusunan skripsi sampai tuntas.
- Pacarku tercinta Ria Piesiskawati yang cerewet dan selalu marah-marah kalau aku sedang malas mengerjakan skripsi dan juga terima kasih atas support dan doa yang selalu kamu berikan untuk ku selama kuliah dan penyusunan skripsi ini, karena

dirimulah aku tetap semangat mengerjakan skripsi ini sampai selesai. Terima kasih ya sayang.

- Buat ketiga kucingku, Chopper, jupe dan pubby yang selalu menghiburku dikala aku sedang setres dengan source code program ku.
- Buat teman-teman sekelasku S1-TI B ' 06, kalian semua adalah teman terbaikku selama aku kuliah. Tak kan aku lupakan saat-saat kuliah bersama kalian.
- dr.Agus kamal Purba.MPH Terima kasih tulang atas support dan nasihat nasihat yang kau berikan kepadaku itu semua sangat membantu dalam penyelesaian skripsi ini dan untuk kehidupanku kedepannya nanti dan juga terima kasih karena telah mendoakan ku dan mensupport diriku sebelum ujian pendadaran karena semua doa dan kata katamu telah membuatku merasa yakin atas kemampuanku.
- Yang terakhir terima kasih buat semua orang yang tidak dapat aku sebutkan satu persatu yang telah membantu dan memberikan doanya kepadaku.

KATA PENGANTAR

Alhamdulillah, puji syukur kehadirat Allah SWT atas limpahan rahmat dan kemudahan-Nya sehingga penulis dapat menyelesaikan laporan skripsi dengan judul Analisis dan Implementasi Enkripsi Basis Data dengan Algoritma Kriptografi Blowfish.

Penulisan Laporan ini dimaksudkan untuk melengkapi salah satu syarat dalam menyelesaikan studi di Jurusan Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta.

Dengan selesainya laporan ini, maka penulis menyampaikan ucapan terima kasih dan penghargaan kepada :

1. Bapak Prof.Dr.M.Suyanto,MM selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Ibu Ema Utami, S.Si, M.Kom selaku Dosen Pembimbing, yang telah banyak meluangkan waktu untuk membimbing dan mengarahkan sehingga skripsi ini dapat terselesaikan.
3. Seluruh Dosen STMIK AMIKOM Yogyakarta yang telah memberikan ilmunya pada penulis.
4. Semua pihak yang selama ini banyak memberi bantuan, dukungan motivasi maupun do'a yang tidak dapat disebutkan satu per satu

Penulis sadar bahwa dalam penyusunan laporan skripsi ini masih banyak yang perlu dikoreksi lebih lanjut, maka penulis dengan senang hati menerima

kritik dan saran demi perbaikan selanjutnya. Semoga laporan ini dapat berperan sebagaimana mestinya.

Yogyakarta, 17 Februari 2010

Penulis

Ari Suhendra

DAFTAR ISI

JUDUL i
PERSETUJUAN ii
PENGESAHAN iii
PERNYATAAN iv
MOTTO v
PERSEMBAHAN vi
KATA PENGANTAR viii
DAFTAR ISI x
DAFTAR TABEL xiv
DAFTAR GAMBAR xv
INTISARI xvii
ABSTRACT xviii
BAB I PENDAHULUAN
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 4
1.6 Metode Penelitian 5
1.7 Sistematika Penulisan Laporan 6
1.8 Jadwal Penelitian 7
BAB II DASAR TEORI
2.1 Dasar Teori 8
2.1.1 Sejarah Kriptografi 8
2.1.2 Konsep Dasar Algoritma Kriptografi 10
2.2 Algoritma Blowfish 16
2.2.1 Sturktur Algoritma Blowfish 17
2.2.2 Enkripsi Algoritma Blowfish 17

2.2.3 Dekripsi Algoritma Blowfish 20
2.2.4 Keamanan Blowfish 21
2.2.5 Kecepatan Kinerja Algortima Blowfish 22
2.3 Basis Data 23
2.3.1 Pengertian Basis Data 23
2.3.2 Database Management System (DBMS) 23
2.3.3 Structure Query Languange (SQL) 24
2.3.4 Keamanan Basis Data 26
BAB III ANALISA DAN PERANCANGAN SISTEM
3.1 Analisis Sistem 28
3.1.1 Identifikasi Permasalahan 28
3.1.1.1 Permasalahan yang Timbul 28
3.1.1.2 Identifikasi Penyebab Masalah 28
3.1.1.3 Titik Keputusan 29
3.1.2 Kebutuhan Perangkat 29
3.1.2.1 Kebutuhan Perangkat keras (Hardware 29
3.1.2.2 Kebutuhan Perangkat Lunak (Software) 30
3.2 Perancangan Sistem 30
3.3 Algoritma Enkripsi 31
3.4 Data Flow Diagram (DFD) 37
3.4.1 DFD Level 0 37
3.4.2 DFD Level 1 38
3.5 Perancangan Form 40
3.5.1 Perancangan Splash Screen 40
3.5.2 Perancangan Menu Utama 40
3.5.3 Perancangan Form Peringatan 42
3.5.4 Perancangan Form About 43
BAB IV IMPLEMENTASI DAN ANALISIS HASIL UJI COBA PROGRAM
4.1 Implementasi Sistem 44
4.1.1 Tampilan Utama 44
4.1.2 Tampilan Masukan (Input) 45

4.1.3 Menu About 47
4.1.4 Proses Enkripsi 48
4.1.5 Proses Dekripsi 50
4.2 Uji Coba Program dan Analisis Hasil 52
4.2.1 Proses enkripsi dengan file sql 52
4.2.2 Proses enkripsi dengan file Gambar 55
4.2.3 Proses enkripsi dengan file Video 56
4.2.4 Proses enkripsi dengan file Suara 57
4.2.5 Proses enkripsi dengan file World 58
4.2.6 Proses enkripsi dengan file Exel 59
4.2.7 Proses enkripsi dengan file Power Point 61
4.2.8 Proses enkripsi dengan file Text 62
4.2.9 Proses enkripsi dengan file PDF 63
4.2.10 Proses dekripsi dengan file sql 64
4.3 Analisis Perbandingan Waktu dan Besaran file 66
4.3.1 Analisis pada file mdf 66
4.3.2 Analisis pada file Gambar 66
4.3.3 Analisis pada file Video 67
4.3.4 Analisis pada file Suara 68
4.3.5 Analisis pada file Dokumen 69
4.3.6 Analisis pada file Exel 70
4.3.7 Analisis pada file Power point 71
4.3.8 Analisis pada file text 72
4.3.9 Analisis pada file PDF 73
4.4 Grafik Analisis Sistem Perbandingan Waktu dan Besaran File 74
4.4.1 Grafik pada file sql 74
4.4.2 Grafik pada file gambar 76
4.4.3 Grafik pada file video 76
4.4.4 Grafik pada file suara 77
4.4.5 Grafik pada file dokumen 77

4.4.6 Grafik pada file exel 78
4.4.7 Grafik pada file power point 78
4.4.8 Grafik pada file text 79
4.4.9 Grafik pada file pdf 79
4.5 Kelebihan dan Kekurangan Sistem 80
4.5.1 Kelebihan Sistem 80
4.5.2 Kekrangan Sistem 80
BAB V PENUTUP
5.1 Kesimpulan 81
5.2 Saran 82
DAFTAR PUSTAKA
LAMPIRAN

DAFTAR TABEL

Tabel 1.1	Jadwal Penelitian	7
Tabel 2.1	Kecepatan Blowfish	22
Tabel 3.1	Simbol-simbol pada flowchart	33
Tabel 3.2	Simbol-simbol pada DFD	39
Tabel 4.1	Perbandingan waktu proses enkripsi dan dekripsi dengan file mdf	66
Tabel 4.2	Perbandingan waktu proses enkripsi dan dekripsi dengan file gambar	66
Tabel 4.3	Perbandingan waktu proses enkripsi dan dekripsi dengan file video	67
Tabel 4.4	Perbandingan waktu proses enkripsi dan dekripsi dengan file suara	68
Tabel 4.5	Perbandingan waktu proses enkripsi dan dekripsi dengan file dokumen	69
Tabel 4.6	Perbandingan waktu proses enkripsi dan dekripsi dengan file excel	70
Tabel 4.7	Perbandingan waktu proses enkripsi dan dekripsi dengan file power point	71
Tabel 4.8	Perbandingan waktu proses enkripsi dan dekripsi dengan file text	72
Tabel 4.9	Perbandingan waktu proses enkripsi dan dekripsi dengan file pdf	73

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Dekripsi 11
Gambar 2.2 Bagan Kriptosistem Secara Umum 12
Gambar 2.3 Algoritma Simetris 14
Gambar 2.4 Proses Enkripsi public key 15
Gambar 2.5 Jaringan Feistel untuk algoritma Blowfish 19
Gambar 2.6 Fungsi F 20
Gambar 2.7 Blok Diagram Dekripsi Blowfish 21
Gambar 3.1 Perancangan Alur Sistem 30
Gambar 3.2 Proses dalam metode BLOWFISH 32
Gambar 3.3 Skema Pembangkitan Kunci 36
Gambar 3.4 DFD Level 0 37
Gambar 3.5 DFD Level 1 38
Gambar 3.6 Rancangan Form Splash 40
Gambar 3.7 Desain Form Interface 41
Gambar 3.8 Desain Form File Kosong 42
Gambar 3.9 Desain Form Password require 42
Gambar 3.10 Desain Form Exit 42
Gambar 3.11 Desain Form About 43
Gambar 4.1 Mnu Utama 44
Gambar 4.2 Tampilan masukan (input) 46
Gambar 4.3 Menu about 47
Gambar 4.4 Isi file skripsi.mdf 52
Gambar 4.5 Skripsi.mdf telah di enkripsi 53
Gambar 4.6 File skripsi.mdf sebelum di enkripsi 53
Gambar 4.7 Skripsi.mdf setelah dienkripsi 54
Gambar 4.8 Amikom.jpg 55
Gambar 4.9 Amikom.jpg enkrip 55
Gambar 4.10 File Video 56
Gambar 4.11 File Video enkrip 56

Gambar 4.12 File suara 57
Gambar 4.13 File suara enkrip 57
Gambar 4.14 File dokumen 58
Gambar 4.15 Form Konversi 58
Gambar 4.16 File dokumen enkrip 59
Gambar 4.17 File excel 59
Gambar 4.18 Form Peringantan 60
Gambar 4.19 File excel enkrip 60
Gambar 4.20 File Power point 61
Gambar 4.21 File Power Point enkrip 61
Gambar 4.22 File text 62
Gambar 4.23 File text enkrip 62
Gambar 4.24 File pdf 63
Gambar 4.25 File pdf enkrip 63
Gambar 4.26 File mdf setelah di enkrip 64
Gambar 4.27 Proses Dekripsi 64
Gambar 4.28 Proses attaching sukses 65
Gambar 4.29 Skripsi.mdf setelah dekrip 65
Gambar 4.30 Grafik besaran file pada percobaan enkripsi file sql 74
Gambar 4.31 Grafik besaran waktu pada percobaan enkripsi file sql 74
Gambar 4.32 Grafik pada percobaan enkripsi file sql 75
Gambar 4.33 Grafik besaran file dan waktu pada file gambar 76
Gambar 4.34 Grafik besaran file dan waktu pada file video 76
Gambar 4.35 Grafik besaran file dan waktu pada file suara 77
Gambar 4.36 Grafik besaran file dan waktu pada file dokumen 77
Gambar 4.37 Grafik besaran file dan waktu pada file excel 78
Gambar 4.38 Grafik besaran file dan waktu pada file power point 78
Gambar 4.39 Grafik besaran file dan waktu pada file text 79
Gambar 4.40 Grafik besaran file dan waktu pada file pdf 79

INTISARI

Seiring dengan perkembangan teknologi dalam dunia bisnis, sistem basis data telah menjadi simbol dari salah satu bentuk aset yang paling berharga. Basis data telah menjadi kebutuhan di beberapa organisasi dan perusahaan komersial pada saat ini seperti bisnis, perbankan, pendidikan, kepegawaian, dan lain-lain. Dengan semakin luasnya penggunaan sistem basis data, perlindungan terhadap informasi yang disimpan dalamnya menjadi sangat diperlukan untuk melindungi dari berbagai macam ancaman diantaranya pembacaan data, manipulasi data dan perusakan data oleh pihak yang tidak berwenang.

Teknik Kriptografi dengan mengunakan algoritma *blowfish* yang di implementasikan dalam suatu bahasa pemrograman dapat mengatasi masalah terjadinya penyalahgunaan terhadap hak akses basis data oleh pihak yang tidak berwenang. Peroses penyandian pada kriptografi terdiri atas dua tahap, yaitu enkripsi dan dekripsi.

Dari hasil pengujian, di dapat bahwa implementasi yang dilakukan di sistem operasi Windows berhasil. Semua jenis file yang telah diuji seperti file Microsoft SQL server (.mdf), Gambar (.jpg, .gif, .bmp, .png, dll), Video (.wmp, .mpeg, .mp4, .avi, .3gp, dll), Suara (.mp3, .wav, .m4a, dll), Microsoft Word (.doc, .docx, .rtf, .txt), Microsoft Excel (.xls, .xlsx), Microsoft PowerPoint (.ppt, .pptx), Text (.txt) dan *Portable Document Format* (.pdf) dapat dilakukan proses enkripsi dan dekripsi.

Kata Kunci: Kriptografi, Algoritma *Blowfish*, Basis data, Keamanan.

ABSTRACT

Along with the development of technology in the business world, the database system has become a symbol of one of the most valuable forms of assets. The database has become a requirement in some organizations and commercial companies at the moment such as business, banking, education, employment, and others. With the increasingly wide use of database systems, the protection of the information stored within it becomes very necessary to protect against a variety of threats such as reading data, data manipulation and destruction of data by unauthorized parties.

Cryptographic techniques by using the blowfish algorithm implemented in a programming language can overcome the abuse of the right of access to the database by unauthorized parties. The process of encoding the cryptography consists of two phases, namely encryption and decryption.

From the test results, it can be done in the implementation of the Windows operating system work. All types of files that have been tested such as Microsoft SQL server files (.mdf), Images (.jpg, .gif, .bmp, .png, etc), Video (.wmp, .mpeg, .mp4, .avi, .3gp, etc.), sound (.mp3,. wav,. m4a, etc), Microsoft Word files (.doc, .docx, .rtf), Microsoft Excel (.xls, .xlsx), Microsoft PowerPoint (. ppt,. pptx), Text (. txt) and Portable Document Format (.pdf) to do the encryption and decryption.

***Keyword**: Cryptography, Blowfish algorithm, database, security.*