

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI BLOWFISH
UNTUK KEAMANAN DOKUMEN
PADA MICROSOFT OFFICE**

SKRIPSI



disusun oleh

Shanty Erikawaty Aryani Tambunan

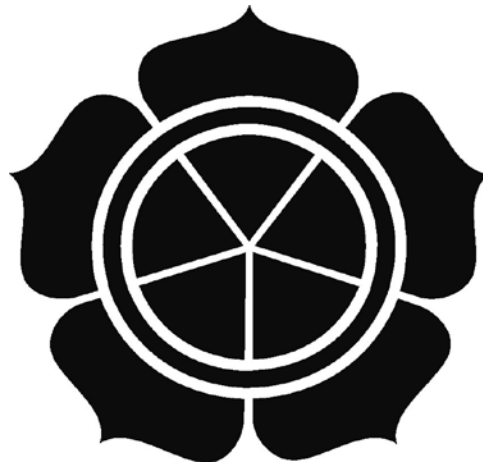
06.11.1189

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2010**

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI BLOWFISH
UNTUK KEAMANAN DOKUMEN
PADA MICROSOFT OFFICE**

Skripsi

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



disusun oleh

Shanty Erikawaty Aryani Tambunan

06.11.1189

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2010**

PERSETUJUAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI BLOWFISH

UNTUK KEAMANAN DOKUMEN

PADA MICROSOFT OFFICE

Yang dipersiapkan dan disusun oleh

Shanty Erikawaty Aryani Tambunan

06.11.1189

Telah disetujui oleh Dosen Pembimbing Skripsi

Pada Tanggal 4 Februari 2010

Dosen Pembimbing,

Ema Utami, S.Si, M.Kom

NIK. 190302037

PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI BLOWFISH UNTUK KEAMANAN DOKUMEN PADA MICROSOFT OFFICE

yang dipersiapkan dan disusun oleh

Shanty Erikawaty Aryani Tambunan
06.11.1189

telah dipertahankan di depan Dewan Penguji
pada tanggal 11 Februari 2010

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

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

Andi Sunyoto, M.Kom
NIK. 190302052

M Rudyanto Arief, MT
NIK. 190302098

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 11 Februari 2010

KETUA STMIK AMIKOM YOGYAKARTA

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

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, dan sepanjang sepengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dah disebutkan dalam daftar pustaka.

Yogyakarta, 22 Februari 2010

Shanty E.A Tambunan

MOTTO

Harga kebaikan manusia adalah diukur menurut apa yang telah dilaksanakan / diperbuatnya. (Ali Bin Abi Thalib)

Manusia tak selamanya benar dan tak selamanya salah, kecuali ia yang selalu mengoreksi diri dan membenarkan kebenaran orang lain atas kekeliruan diri sendiri.

Jenius adalah 1 % inspirasi dan 99 % keringat. Tidak ada yang dapat menggantikan kerja keras. Keberuntungan adalah sesuatu yang terjadi ketika kesempatan bertemu dengan kesiapan. - *Thomas A. Edison*

Kita tidak bisa menjadi bijaksana dengan kebijaksanaan orang lain, tapi kita bisa berpengetahuan dengan pengetahuan orang lain. - *Michel De Montaigne*

Do all the goods you can, All the best you can, In all times you can, In all places you can, For all the creatures you can.

PERSEMBAHAN

Thank's To:

- Allah SWT yang telah memberikan petunjuk-Nya dan kemudahan sehingga skripsi ini dapat selesai dengan baik.
- Kedua Orang Tuaku, terima kasih banyak atas doanya dan semua yang telah diberikan kepadaku. Tanpa kalian aku tidak akan bisa seperti sekarang ini.
- Adik-adikku, Reza A Tambunan dan Rico A Tambunan yang selalu menghiburku dan memberiku semangat.
- Mas Hadi P yang telah memberikan dukungan, semangat dan menemaniku di masa suka dan duka.
- Best Friend ku Tentis Apriana makasih atas doa dan semangat yang diberikan padaku, akhirnya aku akan menyusulmu menjadi sarjana.
- Mas Cahyo & Adit yang telah membantuku menyelesaikan skripsi ini.

- Teman-teman Kosku yang selalu menemaniku dan meramaikan kos : Manik, Rifa (Terima kasih atas pinjaman laptopnya saat pendadaran) & MbK Fio.
- Buat teman-teman sekelasku S1-TI C ' 06, kalian semua adalah teman terbaikku selama aku kuliah. Tak kan aku lupakan saat-saat kuliah bersama kalian.
- Buat teman-teman asisten : Dyah Fajar, Ismi, Gatot, Afif, Rumini, dll terima kasih atas semua doa, semangat dan saran-saran yang diberikan kepadaku.
- 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 kehadiran Allah SWT atas limpahan rahmat dan kemudahan-Nya sehingga penulis dapat menyelesaikan laporan skripsi dengan judul Implementasi Algoritma Kriptografi Blowfish Untuk Keamanan Dokumen Pada Microsoft Office.

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

Dalam proses penyusunan dan penulisan skripsi, penulis menyadari bahwa kemampuan penulis terbatas. Oleh karena itu, penulis menyampaikan terimakasih kepada pihak-pihak yang turut terlibat dari awal proses hingga akhir, antara lain:

1. Bapak Prof.Dr.M.Suyanto,MM selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Bapak Ir.Abas Ali Pangera,M.Kom selaku Ketua Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, S.Si, M.Kom selaku Dosen Pembimbing, yang telah banyak meluangkan waktu untuk membimbing dan mengarahkan sehingga skripsi ini dapat terselesaikan.
4. Bapak Andi Sunyoto, M.Kom dan Bapak M Rudyanto Arief, MT selaku Dosen Penguji, terimakasih atas saran dan kritiknya yang merupakan langkah awal penyempurnaan skripsi ini.

5. Seluruh Dosen STMIK AMIKOM Yogyakarta yang telah memberikan ilmunya pada penulis.
6. Semua pihak yang telah memberikan bantuan kepada penulis yang tidak dapat penulis sebutkan satu persatu.

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

Shanty E.A Tambunan

DAFTAR ISI

JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN.....	iv
MOTTO	v
PERSEMBAHAN.....	vi
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
INTISARI.....	xvii
ABSTRACT.....	xviii
BAB I PENDAHULUAN	
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Metode Penelitian.....	4
1.7 Sistematika Penulisan Laporan	5
1.8 Jadwal Penelitian.....	7

BAB II DASAR TEORI

2.1	Tinjauan Pustaka	8
2.2	Dasar Teori.....	10
2.2.1	Konsep Dasar Kriptografi	10
2.2.2	Algoritma Blowfish.....	15
2.2.3	Kriteria Rancangan Algoritma Blowfish	25
2.2.4	Kecepatan Kinerja Blowfish	26
2.2.5	Bagan Alir (<i>Flow Chart</i>).....	26
2.2.6	Software yang digunakan.....	31

BAB III ANALISA DAN PERANCANGAN SISTEM

3.1	Analisa Perancangan Sistem.....	38
3.1.1	Kebutuhan Perangkat Lunak	38
3.1.2	Strategi Perancangan Perangkat Lunak	39
3.1.3	Deskripsi Perangkat Lunak.....	40
3.2	Perancangan Sistem	41
3.2.1	Flowchart Sistem	41
3.2.2	Diagram Arus Data Sistem / <i>Data Flow Diagram</i> (DFD).....	46
3.3	Perancangan Antar Muka.....	51
3.3.1	Menu Home.....	51
3.3.2	Menu About	53
3.3.3	Menu Tool.....	54
3.4	Perancangan Script Program	56

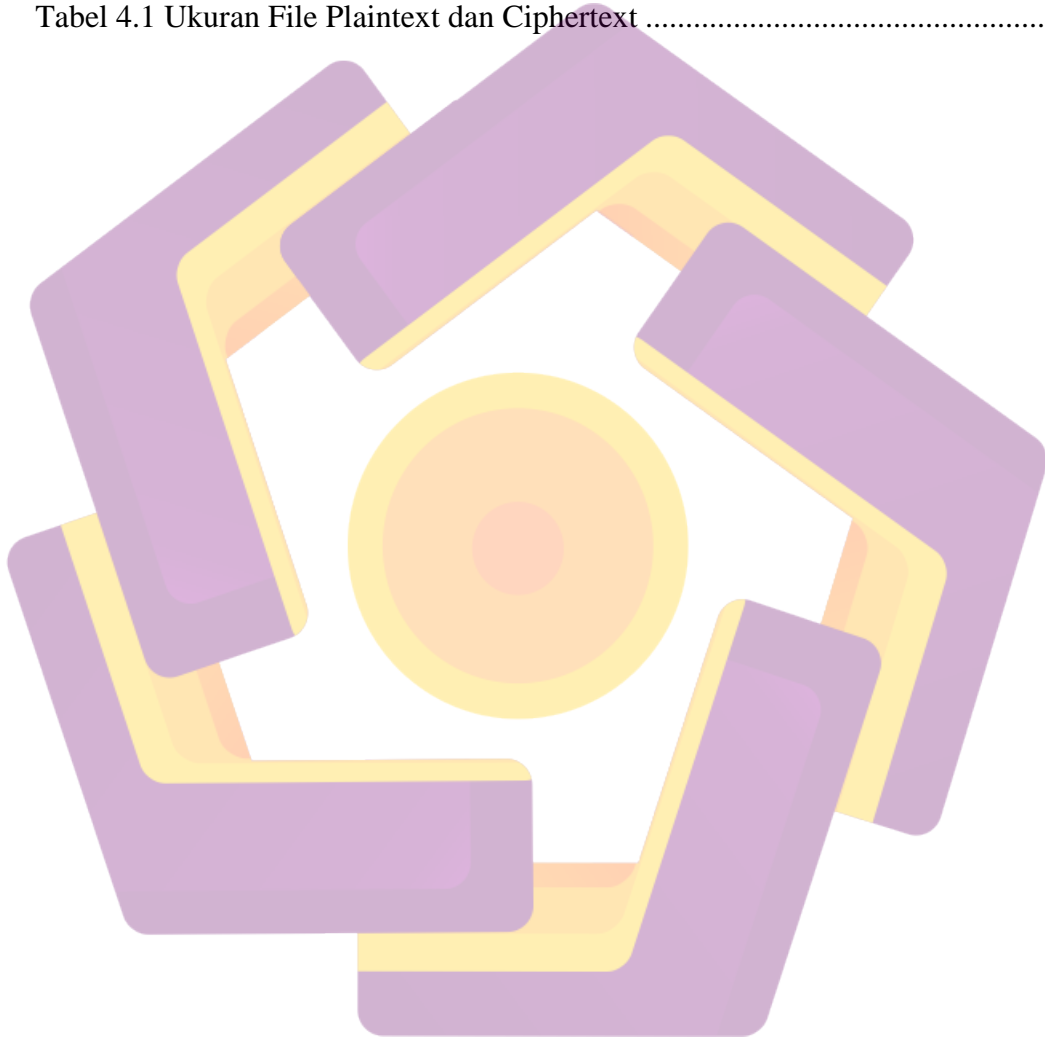
3.4.1	Pendeklarasian variable.....	55
3.4.2	Script enkripsi dan dekripsi.....	56
3.4.3	Inisialisasi array P dan S-box.....	57
BAB IV IMPLEMENTASI DAN UJI COBA PROGRAM		
4.1	Implementasi Sistem.....	76
4.1.1	Menu Home.....	76
4.1.2	Menu About.....	77
4.1.3	Menu Tool.....	78
4.2	Uji Coba Program.....	8
4.2.1	Dasar Uji Coba Rancangan Program.....	80
4.2.2	Tujuan Uji Coba Rancangan Program.....	80
4.2.3	Kesalahan-kesalahan Program.....	81
4.2.4	Simulasi Uji Coba Program dan Hasil.....	82
4.3	Pembahasan Masalah.....	111
5.3.1	Ukuran File.....	111
5.3.2	Kinerja Sistem.....	112
BAB V PENUTUP		
5.1	Kesimpulan.....	114
5.2	Saran.....	116

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR TABEL

Tabel 1.1 Jadwal Pelaksanaan.....	7
Tabel 2.1 Kecepatan Blowfish	26
Tabel 4.1 Ukuran File Plaintext dan Ciphertext	111



DAFTAR GAMBAR

Gambar 2.1 Bagan Kriptosistem secara Umum	12
Gambar 2.2 Proses Enkripsi Konvensional	14
Gambar 2.3 Proses Enkripsi <i>Public Key</i>	15
Gambar 2.4 Blok Diagram Algoritma Blowfish dalam Jaringan Feistel	19
Gambar 2.5 Flowchart Algoritma Blowfish	20
Gambar 2.6 Fungsi F	22
Gambar 2.7 Flowchart Fungsi F	22
Gambar 2.8 Blok Diagram Dekripsi Blowfish	24
Gambar 2.9 Tampilan Awal Microsoft Visual Basic 6.0	32
Gambar 2.10 Main Window	32
Gambar 2.11 Form Window	33
Gambar 2.12 Toolbox Window	33
Gambar 2.13 Properties Window	34
Gambar 2.14 Form Layout Window	34
Gambar 2.15 Project Window	35
Gambar 3.1 Flowchart Sistem	42
Gambar 3.2 Flowchart Fungsi F	44
Gambar 3.3 Flowchart Proses Enkripsi dan Dekripsi	45
Gambar 3.4 Diagram Kontext	47
Gambar 3.5 DFD Level 0	48
Gambar 3.6 DFD Level 1.1	49

Gambar 3.7 DFD level 1.2	50
Gambar 3.8 Rancangan Menu Utama	52
Gambar 3.9 Rancangan Menu About	53
Gambar 3.10 Rancangan Menu Awal Folder Lock.....	54
Gambar 3.11 Rancangan Menu Utama Folder Lock.....	54
Gambar 3.12 Rancangan Menu Ganti Password Folder Lock.....	55
Gambar 4.1 Menu Utama	77
Gambar 4.2 Menu About.....	78
Gambar 4.3 Menu Awal Folder Lock	78
Gambar 4.4 Menu Utama Folder Lock	79
Gambar 4.5 Menu Mengganti Password Folder Lock	79
Gambar 4.6 Hasil Enkripsi Pertama	83
Gambar 4.7 Hasil Enkripsi Kedua.....	84
Gambar 4.8 Plaintext blowfish.txt.....	85
Gambar 4.9 Ciphertext file blowfish.txt.....	86
Gambar 4.10 Plaintext Bentuk normal chomsky.doc.....	87
Gambar 4.11 Ciphertext Bentuk normal chomsky.doc	88
Gambar 4.12 Plaintext Blowfish.docx	89
Gambar 4.13 Blowfish.docx.....	90
Gambar 4.14 Plaintext Manfaat Tidur.rtf.....	91
Gambar 4.15 Ciphertext Manfaat Tidur.rtf	92
Gambar 4.16 Plaintext nama.ppt	93
Gambar 4.17 Ciphertext nama.ppt	94

Gambar 4.18 Plaintext ITStrategy.pptx.....	95
Gambar 4.19 Hasil enkripsi file .pptx	96
Gambar 4.20 Plaintext Risk Assesment Template.Xls	97
Gambar 4.21 Ciphertext Risk Assesment Template.Xls.....	98
Gambar 4.22 Plaintext jadwal_ujian.xlsx	99
Gambar 4.23 Ciphertext jadwal_ujian.xlsx.....	100
Gambar 4.24 Plaintext rumah_sakit.mdb.....	101
Gambar 4.25 Ciphertext rumah_sakit.mdb	102
Gambar 4.26 Proses Dekripsi.....	103
Gambar 4.27 Peringatan jika berhasil dekripsi	104
Gambar 4.28 Hasil Dekripsi.....	104
Gambar 4.29 Masukkan Password Lock Folder	105
Gambar 4.30 Memilih File yang akan dikunci.....	106
Gambar 4.31 Menganti Password Lock Folder.....	106
Gambar 4.32 Listing Program 16 putaran	107
Gambar 4.33 Hasil Enkripsi dengan 16 Putaran	108
Gambar 4.34 Listing Program 10 putaran.....	108
Gambar 4.35 Hasil Enkripsi dengan 10 Putaran	109
Gambar 4.36 Listing Program 20 putaran	109
Gambar 4.37 Hasil Enkripsi dengan 20 Putaran	110

INTISARI

Masalah keamanan merupakan salah satu aspek paling penting dalam dunia teknologi informasi, misalnya : keamanan dokumen. Sekarang ini, sebagian besar dokumen-dokumen menggunakan aplikasi Microsoft Office. Untuk mengatasi masalah keamanan dokumen ini, penulis melakukan pendekatan teknologi enkripsi data menggunakan algoritma Blowfish. Enkripsi data merupakan teknologi untuk memastikan bahwa informasi yang mengalir pada suatu sesi tidak disadap atau diubah orang lain. Blowfish atau sering disebut "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem*, yaitu menggunakan kunci yang sama untuk enkripsi dan dekripsinya.

Penelitian ini dibagi menjadi 2 tahap. Pertama adalah implementasi dari algoritma *Blowfish* dalam bahasa pemrograman Visual Basic 6.0 menjadi sebuah model kriptosistem berbasis desktop. Dilanjutkan dengan menguji kunci dan beberapa ekstensi file Microsoft Office yang berbeda, serta pengujian terhadap *tool* tambahan berupa *Lock Folder* yang berguna untuk mengunci folder.

Dari hasil pengujian, di dapat bahwa implementasi yang dilakukan di sistem operasi Windows berhasil. Semua jenis file Microsoft Office meliputi file Microsoft Word (.doc, .docx, .rtf, .txt), Microsoft Excel (.xls, .xlsx), Microsoft Access (.mdb) dan Microsoft PowerPoint (.ppt, .pptx) dapat dilakukan proses enkripsi dan dekripsi.

Kata Kunci: Kriptografi, Algoritma *Blowfish* , Microsoft Office, *Symmetric Cryptosystem*, informasi rahasia.

ABSTRACT

Security problem is one of the most important aspect in the world of information technology, such as: security of documents. Today, most of the documents using Microsoft Office applications. To overcome the security problems of this document, the author approaches the data encryption technology using Blowfish algorithm. A data encryption technology to ensure that the information that flows in a session is not intercepted or modified others. Blowfish or often called "OpenPGP.Cipher.4" is a Symmetric Cryptosystem, using the same key for encryption and decryption.

This research is divided into 2 part. The first is the implementation of the Blowfish algorithm in the programming language Visual Basic 6.0 to be a desktop model based Cryptosystem. The Second thing is testing key and several Microsoft Office file extensions, and testing of additional tools useful Folder Lock to lock the folder.

The result said that the implementation in Windows operation system is successful. All Microsoft Office file types including Microsoft Word files (. Doc,. Docx,. Rtf,. Txt), Microsoft Excel (. Xls,. Xlsx), Microsoft Access (. Mdb) and Microsoft PowerPoint (. Ppt,. Pptx) can do encryption and decryption process

Keyword: *Cryptography, Blowfish Algorithm, Microsoft Office, Symmetric Cryptosystem, Secret Information.*