

**PENGEMBANGAN *PROTOTYPE* SISTEM KRIPTOGRAFI UNTUK
ENKRIPSI DAN DEKRIPSI DATA *OFFICE* MENGGUNAKAN
METODE BLOWFISH DENGAN BAHASA PEMROGRAMAN JAVA**

TESIS



**Oleh:
Mohamad Natsir
1111601520**

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2014**

**PENGEMBANGAN *PROTOTYPE* SISTEM KRIPTOGRAFI UNTUK
ENKRIPSI DAN DEKRIPSI DATA *OFFICE* MENGGUNAKAN
METODE BLOWFISH DENGAN BAHASA PEMROGRAMAN JAVA**

TESIS

Diajukan sebagai salah satu persyaratan
untuk mendapatkan gelar Magister Ilmu Komputer (MKOM)



Oleh:
Mohamad Natsir
1111601520

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2014**



PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini,

Nama Mahasiswa : MOHAMAD NATSIR
Nomor Induk Mahasiswa : 1111601520
Program Studi : MAGISTER ILMU KOMPUTER
Konsentrasi : REKAYASA KOMPUTASI TERAPAN
Fakultas/Program : PASCASARJANA

menyatakan bahwa **TESIS** yang berjudul :
PENGEMBANGAN PROTOTYPE SISTEM KRIPTOGRAFI UNTUK ENKRIPSI
DAN DEKRIPSI DATA OFFICE MENGGUNAKAN METODE BLOWFISH
DENGAN BAHASA PEMROGRAMAN JAVA.

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. Saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan apabila di kemudian pernyataan ini tidak benar.

Jakarta, 03 Maret 2014



(MOHAMAD NATSIR)



**PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PENGESAHAN

Nama Mahasiswa : Mohamad Natsir
Nomor Induk Mahasiswa : 1111601520
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Juduk Tesis : Pengembangan *Prototype* Sistem Kriptografi
untuk Enkripsi dan Dekripsi *Data Office Menggunakan* Metode *Blowfish* dengan
Bahasa Pemrograman JAVA

Jakarta, 03 Maret 2014

Tim Penguji:

Tanda Tangan:

Ketua,
Ir. Wendi Usino, M.M., M.Sc., Ph.D

Anggota,
Hadi Syahrial, M.M., M.Kom

Pembimbing,
Dr. Ir. Nazori Az, M.T

Ketua Program Studi

Dr. Ir. Nazori Az, M.T

ABSTRAK

Perkembangan teknologi komputer yang semakin pesat menjadikan komputer banyak dijumpai mulai dari instansi pemerintahan, perumahan, sekolah-sekolah, warung internet, rumah tangga, bahkan personal atau yang disebut dengan laptop menjadikan komputer sebagai kebutuhan untuk semua kalangan. Pekerjaan-pekerjaan yang dahulunya manualpun kini mulai banyak yang terkomputerisasi mulai dari pekerjaan rumah dari sekolah hingga perusahaan-perusahaan bertaraf internasional dan semua pekerjaan-pekerjaan itu adalah sebuah informasi penting. Layaknya informasi penting, sistem pengamanan adalah bagian krusial dari suatu aplikasi komputer dan salah satu cara untuk melindungi data kita dari pihak-pihak tidak bertanggung jawab adalah dengan melakukan kriptografi seperti yang akan penyusun pakai yaitu menggunakan algoritma *blowfish*. *Blowfish* atau *OpenPGP.Cipher.4* merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem*, metode enkripsinya mirip dengan Data Enkripsi Standar (DES-like-Cipher). Dibuat untuk digunakan pada komputer yang mempunyai *microprocessor* besar (32-bit keatas dengan cache data yang besar). *Blowfish* dikembangkan untuk memenuhi kriteria desain yang cepat dalam implementasinya dimana pada keadaan optimal dapat mencapai 26 *clock cycle* perbyte, kompak dimana dapat berjalan pada memori kurang dari 5 KB, sederhana dalam algoritmanya sehingga mudah diketahui kesalahannya, dan keamanan yang variable dimana panjang kunci bervariasi (minimum 32 bit, maksimum 448 bit, Multiple 8 bit, *default* 128 bit).

Kata kunci: kriptografi, key simetrik, algoritma *blowfish*, enkripsi, dekripsi

ABSTRACT

The development of computer technology that makes computers much more rapidly found from government agencies, housing, schools, internet cafes , household , personal or even called to make a laptop computer as a requirement for all circles . The works were formerly manual now vastly computerized ranging from homework from school to international companies and all the jobs it is an important information. Like the important information , the security system is a crucial part of a computer application and one way to protect our data from the parties is irresponsible to perform cryptographic would like to use that compiler uses blowfish algorithm. Blowfish or OpenPGP.Cipher.4 is included in the class encryption Symmetric Cryptosystem, the encryption method is similar to the Data Encryption Standard (DES - like - Cipher). Created for use on computers that have a large microprocessor (32 - bit or more with large data caches) . Blowfish was developed to meet the design criteria allows the implementation where the optimal state can reach 26 clock cycles perbyte compact, which can run on less than 5 KB of memory , the simple algorithm so easy to determine guilt, and the security which the variable key length varies (minimum 32 bits, 448 bits maximum, Multiple 8 bits, 128 bits default).

Key words : cryptography,symmetric key, blowfish algorithm, encryption, decryption

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Dengan kerendahan hati penulis panjatkan puji dan syukur yang sedalam-dalamnya kepada Allah SWT Sang Pencipta semesta alam, karena hanya dengan rahmat dan karunia-Nya-lah naskah akhir tesis yang berjudul "PENGEMBANGAN *PROTOTYPE* SISTEM KRIPTOGRAFI UNTUK ENKRIPSI DAN DEKRIPSI DATA *OFFICE* MENGGUNAKAN METODE BLOWFISH DENGAN BAHASA PEMROGRAMAN JAVA" ini dapat diselesaikan. Shalawat serta salam senantiasa tercurahkan kepada Rasulullah yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu. Dalam penyusunan naskah akhir tesis ini, penulis ingin menyampaikan ucapan terimakasih kepada:

1. Allah SWT, atas segala rahmat dan ridho-Nya yang selalu menyertai seluruh aktivitas penulis;
2. Ibuku, Ka Ely, Ka Zainal, Ka Zul, yang senantiasa memberikan kasih sayang, nasihat, dukungan semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir.
3. Istriku Roswita dan kedua anak saya Rizky dan Nazwa, yang selalu memberikan kebahagiaan dan keceriaan.
4. Bapak Dr. Ir. Nazori AZ, MT, selaku pembimbing yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini;
5. Bapak Dr. Moedjiono, M.Sc, selaku Direktur Program Pascasarjana yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini;
6. Serta semua pihak yang tidak dapat dituliskan.

Sebagai seorang manusia yang selalu memiliki kekurangan, penulis menyadari bahwa naskah akhir tesis ini masih banyak kekurangan. Oleh karena itu demi menyempurnakan naskah tesis ini, segala bentuk saran dan kritik mohon dapat dikirimkan melalui *e-mail* ke alamat mohnatsir2011@yahoo.co.id.

Wassalamu'alaikum. Wr. Wb.

Jakarta, Januari 2014

M. Natsir

DAFTAR ISI

	Halaman
ABSTRAK.....	i
KATA PENGANTAR.....	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL.....	vii
BAB I PENDAHULUAN.....	1
I.1 Latar Belakang.....	1
I.2 Masalah Penelitian.....	4
I.2.1. Identifikasi Masalah	4
I.2.2. Pembatasan Masalah	4
I.2.3. Rumusan Masalah	4
I.3. Tujuan dan Manfaat Penelitian.....	5
I.3.1. Tujuan Penelitian.....	5
I.3.2. Manfaat Penelitian.....	5
I.4. Tata Urut Penulisan	5
I.5. Daftar Pengertian	7
BAB II LANDASAN PEMIKIRAN	9
2.1 Tinjauan Pustaka	9
2.1.1. Keamanan Informasi.....	9
2.1.2. Aspek – Aspek Keamanan Informasi.....	10
2.1.3. Aspek-aspek Ancaman Informasi.....	10
2.1.3.1 Interruption.....	10

2.1.3.2 Interception.....	11
2.1.3.3 Modification	11
2.1.3.4 Fabrication.....	11
2.1.4. Strategi Keamanan Informasi	12
2.1.4.1 Physical Security	12
2.1.4.2 Personal Security	12
2.1.4.3 Operasional Security	12
2.1.4.4 Communication Security	12
2.1.4.5 Network Security.....	13
2.2 Kriptografi	13
2.2.1 Definisi Kriptografi	13
2.2.2 Terminologi dalam Kriptografi	15
2.2.3 Konsep Matematis Algoritma Kriptografi	24
2.2.4 Tujuan Kriptografi.....	16
2.2.5 Pembabakan Kriptografi.....	17
2.2.6 Kriptografi Sistem Simetris.....	18
2.2.7 Algoritma Blowfish.....	22
2.2.7.1 Blok Blowfish	23
2.2.7.2 Key-Expansion.....	32
2.2.8 Enkripsi Data	25
2.2.9 Dekripsi Data.....	27
2.2.10 Pembangkitan Subkunci	29
2.2.11 Skema Diagram Algoritma Blowfish	30
2.2.12. Object Oriented Programming (OOP) Bahasa JAVA.....	32
2.2.12.1 Sejarah Perkembangan Java.....	32

2.2.12.2	Versi Awal	34
2.2.12.3	Kelebihan	34
2.2.12.3.1	Kelebihan Utama	34
2.2.12.3.2	Perpustakaan Kelas Yang Lengkap	35
2.2.12.3.4	Bergaya C++	35
2.2.12.3.5	Pengumpulan Sampah Otomatis	35
2.2.13	Kekurangan	36
2.2.13.1	Kurangnya Kompatibilitas Antar Platform	36
2.2.13.2	Mudah di Dekompilasi	36
2.2.13.3	Penggunaan Memori yang Banyak	36
2.2.14	Pengertian Pemrograman Java Netbeans	37
2.2.14.1	Fitur-Fitur dari Platform Netbeans	37
2.2.14.2	Fitur-Fitur yang terdapat dalam Netbeans	38
2.2.15	Model Pengembangan Sistem dengan Metode Waterfall	39
2.2.16	Flow Chart	43
2.3	Tinjauan Studi	45
2.4	Tinjauan Obyek Penelitian	50
2.4.1	Perangkat Keras	51
2.4.2	Perangkat Lunak	51
2.5	Pola Pikir	52
2.6	Hipotesis	56
BAB III	DESAIN PENELITIAN	57
3.1	Jenis Penelitian	57
3.2	Metode Pemilihan Sampel	57
3.3	Metode Pengumpulan Data	57

3.4 Instrumentasi	58
3.5 Teknik Perancangan, Implementasi, dan Pengujian	58
3.5.1 Implementasi.....	59
3.5.2 Pengujian Sistem	59
3.5.3 Langkah-Langkah Penelitian	60
3.5.4 Perumusan Masalah	61
3.5.5 Studi Kepustakaan	61
3.5.6 Memformulasikan Hipotesis.....	61
3.5.7 Perancangan Aplikasi	62
3.5.8 Pengujian Sistem.....	62
3.5.9 Rencana Implementasi.....	62
3.5.10 Pengujian dan Analisis	63
3.5.11 Penarikan Kesimpulan	63
3.5.11 Jadwal Penelitian	64
BAB IV PEMBAHASAN HASIL PENELITIAN	66
4.1 Analisis Sistem.....	66
4.1.1 Analisa Masalah.....	66
4.1.2 Temuan dan Interpretasi	67
4.1.3 Perubahan Plaintext dan Key menjadi Biner	67
4.1.4 Enkripsi Algoritma Blowfish.....	68
4.1.5 Perancangan Sistem	73
4.2 Perancangan Layar Aplikasi	74
4.2.1 Layar Menu Utama	74
4.2.2 Layar Menu Enkripsi	75
4.2.3 Layar Menu Dekripsi	79

4.3 Pengujian Sistem.....	82
4.3.1 Pengujian <i>Black Box</i>	82
4.4 Implikasi Penelitian.....	83
4.4.1 Aspek Sistem	84
4.4.2 Aspek Penelitian Lanjut.....	84
BAB V KESIMPULAN DAN SARAN.....	86
5.1 Kesimpulan	86
5.2 Saran.....	87
DAFTAR PUSTAKA.....	88
LAMPIRAN-LAMPIRAN.....	93

DAFTAR GAMBAR

Gambar	Halaman
II-1 Aspek-aspek Ancaman Informasi.....	21
II-2 Skema enkripsi dan dekripsi dengan kunci.....	16
II-3 Struktur Blok Cipher.....	20
II-4 Blok Diagram Algoritma Enkripsi <i>Blowfish</i>	26
II-5 Fungsi F dalam <i>Blowfish</i>	27
II-6 Blok Diagram Algoritma Dekripsi <i>Blowfish</i>	28
II-7 Skema Fungsi F Algoritma <i>Blowfish</i>	30
II-8 Skema Diagram Algoritma <i>Blowfish</i>	31
II-9 Tahapan Pengembangan Sistem dengan Metode Waterfall.....	40
II-8 Pola Pikir.....	53
II-9 Kerangka Konsep Proses Enkripsi Data Office pada Aplikasi.....	54
II-10 Kerangka Konsep Proses Dekripsi Data Office pada Aplikasi.....	55
III-1 Langkah-Langkah Penelitian.....	60
IV-1 Flow Chart Susunan Program.....	74
IV-2 Tampilan Menu Utama Aplikasi.....	75
IV-3 Tampilan Layar <i>Select File</i> di <i>Folder</i>	77
IV-4 Tampilan Layar Menu <i>Enter Key</i>	77
IV-5 Tampilan Layar Menu <i>Encrypting</i>	78
IV-6 Flow Chart Proses <i>Encrypt</i>	79
IV-7 Tampilan Layar Menu <i>Enter Key Decrypt</i>	80
IV-8 Tampilan Layar Menu Proses Derypting.....	81
IV-9 Flow Chart Proses Decrypt.....	81

DAFTAR TABEL

Tabel		Halaman
II-1	Simbol Flow Chart.....	44
II-2	Ringkasan Tinjauan Studi.....	48
III-1	Jadwal Penelitian.....	64
IV-1	Hasil Pengujian <i>file office</i>	82
IV-2	Hasil Pengujian <i>Blackbox</i>	83



CERDAS BERBUDI LUHUR

DAFTAR PUSTAKA

- [Andriyansah 2005] Andriyansyah. Perangkat Lunak Keamanan Data menggunakan metode Blowfish dan metode RC4, Jakarta, 2005.
- [Ariyus 2006] Ariyus, Dony. Computer Security, Yogyakarta : 2006.
- [Ariyus 2008] Ariyus, Dony. Pengantar Ilmu Kriptografi : Teori, Analisis, dan Implementasi. Andi, Yogyakarta, 2008.
- [Ariyus 2009] Ariyus. Keamanan Data dan Komunikasi. Penerbit Graha ilmu, Yogyakarta: 2009 [Diakses 08 November 2013].
- [Asep 2010] Asep, Herman, Suyanto. Pemrograman Java: Konsep Pemrograman Berorientasi Objek. < <http://www.bambutechno.com> > (Diakses 22 Januari 2014).
- [Aziz 2013] Abdul Aziz. Implementasi Setganografi Teknik LSB (Least Significant Bit) dengan Algoritma Kriptografi Blowfish dan Fungsi Hash SHA-1: 2013.
- [Burnett 2004] Burnett, Steve and Raine, Stephen. RSA Security's Official Guide to Cryptography. Mc Graw Hill Osborn, California: 2004.
- [Christian 2009] Christian, W. Dawson, Projects in Computing and Information Systems. < www.pearsoned.co.uk > England. First published : 2005 (Diakses 13 Maret 2013).